

Manual del Usuario

Abril, 2012

Tabla de Contenidos

Instalación del Hardware

Advertencias

- No trabaje en el sistema o conecte o desconecte los cables durante la operación del dispositivo.

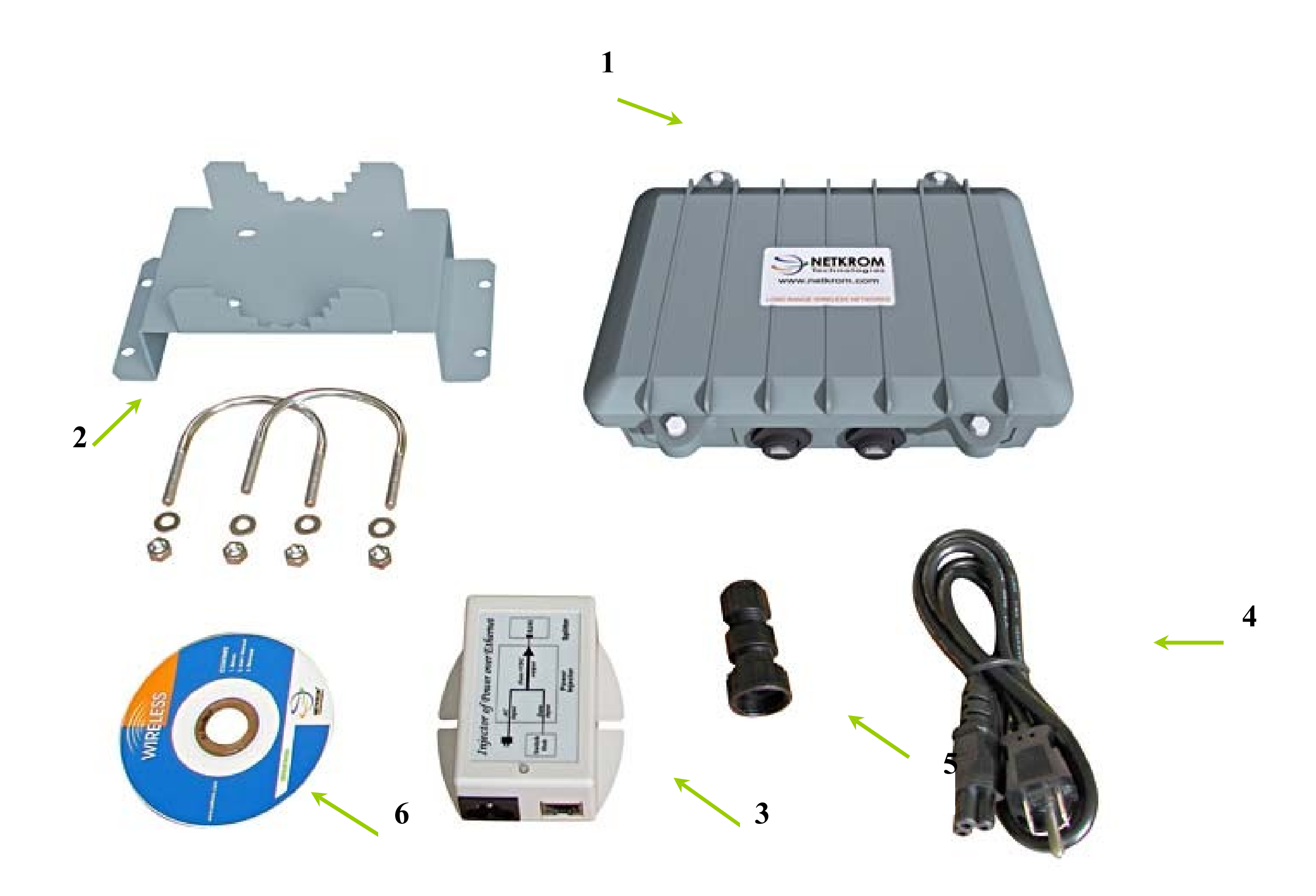
- No coloque la antena cerca de líneas de tensión u otros circuitos eléctricos. Cuando instales la antena tome mucho cuidado de no entrar en contacto con dichos circuitos ya que podrían causarle serias lesiones o incluso la muerte.

- Para cumplir con las reglas de regulación, el radio y la antena externa deben ser profesionalmente instalados. El administrador de red u otro profesional de telecomunicaciones responsable de la instalación y configuración del equipo debe ser un instalador profesional adecuado. Después de la instalación, el acceso al dispositivo debería ser protegido con una contraseña por el administrador de red para así mantener el cumplimiento regulatorio.

- El WaveKROM Backhaul 2000 y el inyector PoE pueden ser dañados por la aplicación incorrecta de energía eléctrica. Leas y siga cuidadosamente las instrucciones antes de conectar el sistema a su fuente de energía eléctrica.

Contenido del Paquete

Tómese un momento para asegurarse que usted tenga todas las partes de su kit antes de empezar a instalar el producto. Si alguna de las partes falta, por favor contáctese con su vendedor local o contáctenos.



Contenido del Kit

1. Dos unidades WaveKrom Backhaul 2000 Series.

2. Soportes (incluye:, 2 soportes y 4 tuercas)

3. Inyector PoE 100-240VAC – 18VDC, 350 mA

4. Cable de alimentación

5. Sistema de conectores RJ45 resistentes al agua

6. CD ROM

Requisitos para la Instalación

Antes de empezar, por favor verifique que lo siguiente esté disponible:

- Cable Ethernet CAT5/5e o FTP (desde el WaveKROM Backhaul 2000 al inyector PoE)
- Al menos una computadora que tenga instalado el NMS y una tarjeta de red alámbrica o inalámbrica.
- Que la gama de protocolos TCP/IP estén correctamente instalados y configurados.

¡Importante!

- configure y verifique el funcionamiento del WaveKROM Backhaul 2000 antes de instalar la unidad en un lugar remoto.
- Usted podría necesitar instalar un arrestor de rayos para proteger su WaveKROM Backhaul 2000 de descargas eléctricas.
- Para elegir la mejor ubicación para su WaveKROM Backhaul 2000 elija un lugar elevado donde árboles, edificios y largas estructuras de acero no obstruyan la señal de la antena y además que ofrezca una máxima propagación de línea de vista con los usuarios.
- Seleccione una antena apropiada para mejorar el rango y cobertura. Además el WaveKROM Backhaul 2000 le permite ajustar parámetros como la potencia de transmisión para lograr mejores resultados.

Instalación del WaveKROM Backhaul 2000

El siguiente diagrama muestra la configuración general del WaveKROM Backhaul 2000.



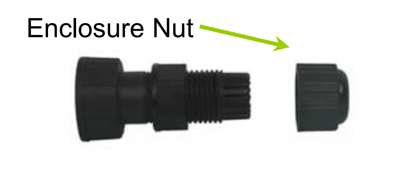
Paso 1:

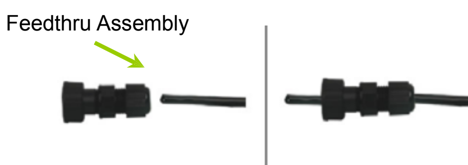
Conecte su cable Ethernet UTP o al conector RJ-45 del WaveKROM Backhaul 2000. Luego conecte el otro extreme del cable al inyector PoE.

Para el PoE Netkrom, la longitud recomendada del cable CAT 5 es de hasta 80 metros.

1. – Retire la cubierta del feedthru. Esta puede ser desechada.

2. – Inserte el conector RJ45 a través del feedthru





3. – Apriete el compression nut suavemente al feedthru



4. – Inserte el conector rj45 al Puerto Ethernet del WaveKROM Backhaul 2000.



5. – Finalmente ajuste y enrosque el sistema adecuadamente.



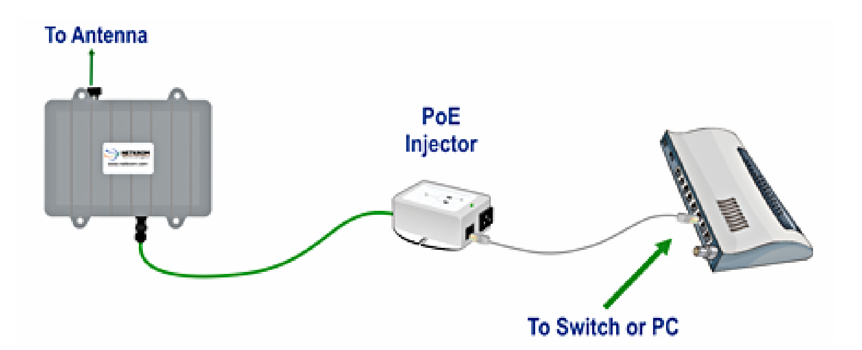
Paso 2:

Conecte la antena externa al conector N hembra del WaveKROM Backhaul 2000.



Paso 3

Conecte un cable Ethernet desde el Netkrom PoE hasta un switch o una PC, conecte otro cable Ethernet desde el PoE hasta el WaveKROM Backhaul 2000.



Nota:

El cable Cat.5 usado entre el Puerto Ethernet del PoE etiquetado con el mensaje WARNING y el WaveKROM Backhaul 2000 debe ser un cable directo.

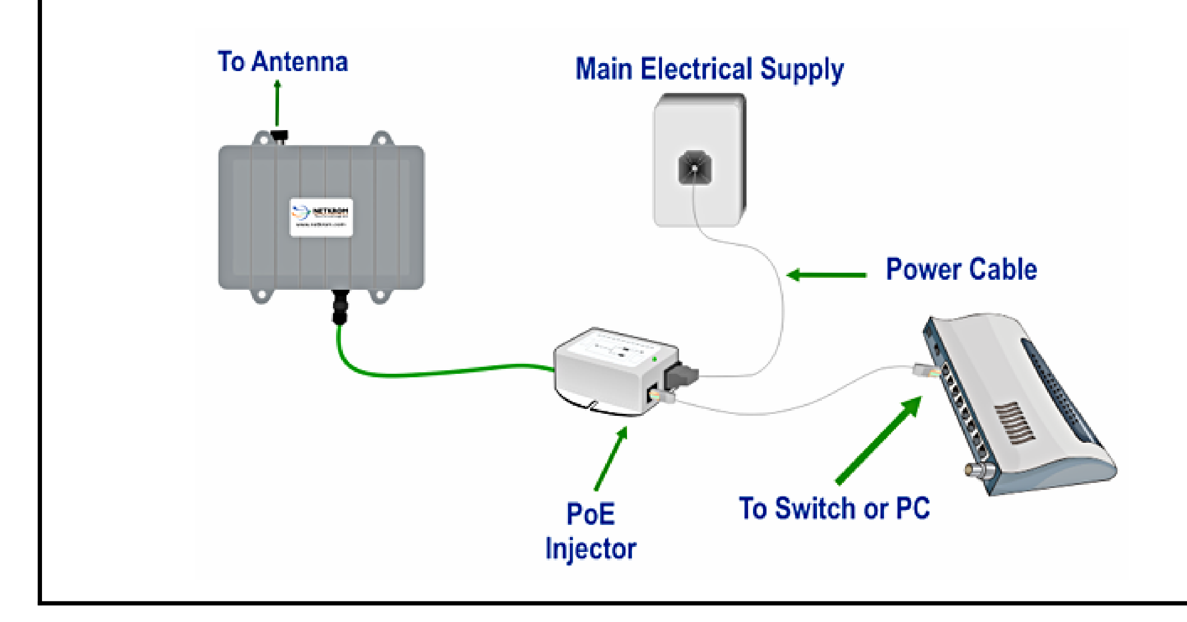
El cable Cat.5 usado entre el puerto Ethernet del PoE etiquetado con “Switch Hub” y el switch puede ser directo o cruzado.

El cable Cat.5 usado entre el puerto Ethernet del PoE etiquetado con “Switch Hub” y la PC debe ser cruzado.

Conecte el cable de alimentación suministrado en el Netkrom PoE kit a la fuente principal de energía eléctrica y el conector del cable de alimentación al socket del PoE.
Ahora encienda la fuente de alimentación. Note que el POWER LED (LED de Encendido) se ha prendido.
Esto indica que el WaveKROM Backhaul 2000 está recibiendo energía a través del PoE Netkrom y que la conexión entre su WaveKROM Backhaul 2000 y su red se ha establecido satisfactoriamente.

Nota:

Por favor use el adaptador de corriente suministrado en el paquete. Usar un adaptador diferente con un voltaje diferente dañará el producto.



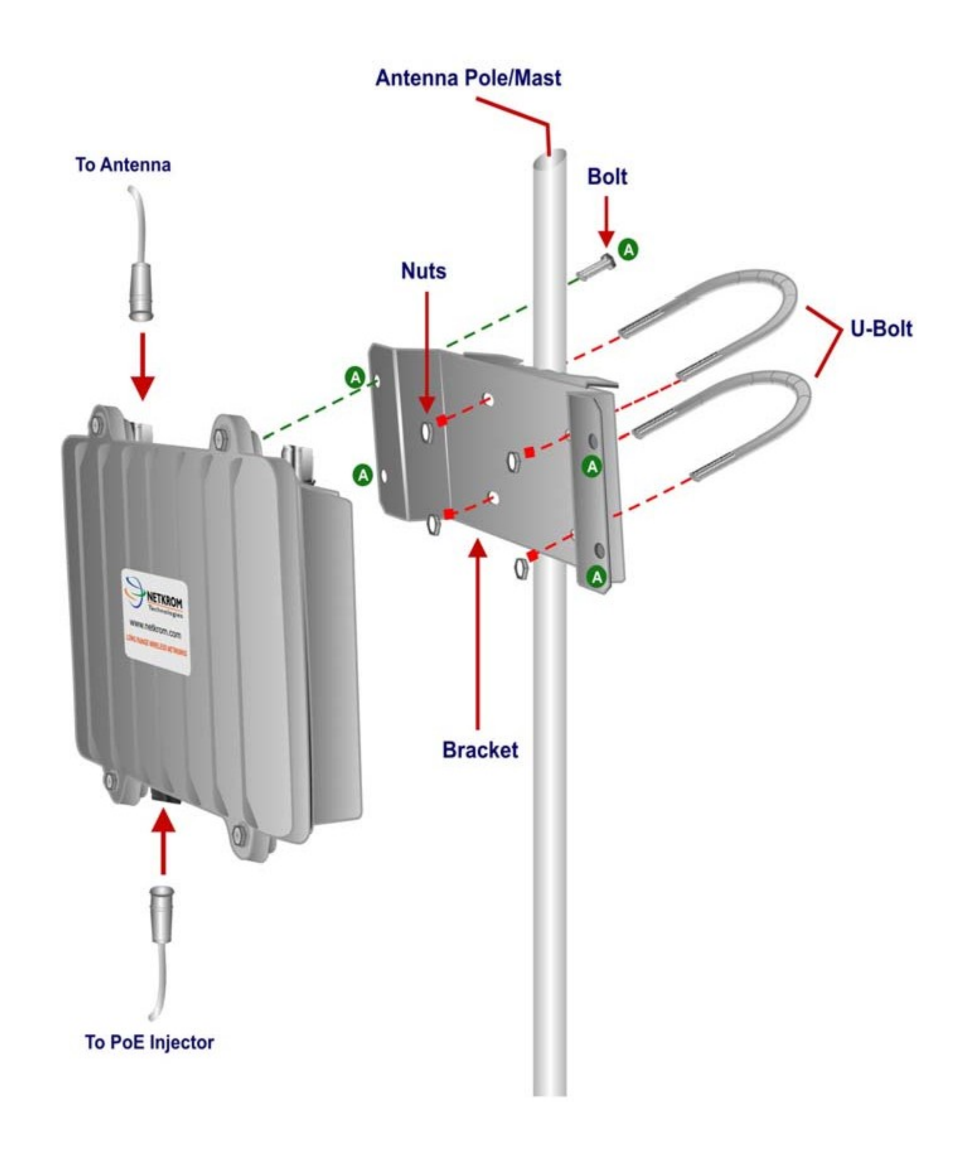
Montaje del WaveKROM Backhaul 2000 en un Mástil o Torre

El WaveKROM Backhaul 2000 puede ser montado en un mástil o una torre como se muestra a continuación:

1. – Monte el soporte al mástil con los pernos en forma de U.

2. – coloque el WaveKROM Backhaul 2000 al soporte que ya se encuentra montado en el mástil con los tornillos y pernos en forma de U suministrados en el paquete.

3. – Apriete y ajuste los pernos en forma de U y tornillos con herramientas de mano.



1. Descripción del Producto

El **NETKROM Network Management System (NNMS)** es utilizado para configurar y administrar redes inalámbricas de los nodos de **NETKROM** como el WaveKROM Backhaul 2000. El NETKROM NMS ha sido diseñado para suministrar a los administradores de red una forma simple y with a comprensiva de controlar y configurar sus nodos de red.

1.1 Compatibilidad y Requisitos

El software NETKROM NMS funciona el cualquier PC o Mac soportado por JAVA. Es decir, cualquier versión de Microsoft Windows (98/ME/2000/NT/XP/VISTA) o GNU/Linux.

1.2 Características del NETKROM NMS

- Protocolo de comunicación avanzada entre el software de Netkrom y el NETKROM NMS alcanzando altos niveles de interactividad. Adicionalmente un esquema de encriptación segura le garantiza una configuración y monitoreo seguro de los nodos NETKROM.
- Configuración sencilla de Hot-Spot.
- Configuración sencilla de WISP.
- Nuevas herramientas de estadísticas basadas en gráficos el cual permite ver la utilización del ancho de banda en tiempo real por interfaz de red.
- Capaz de mostrar topologías de red más robustas.
- Soporta la capacidad de Multi Router Traffic Grapher (MRTG)

1.3 Características NETKROM

- Mecanismos de fallas avanzadas los cuales garantizan la estabilidad del nodo
- Funciones avanzadas de Hostpot
- Re direccionamiento web (Método de acceso universal)
- Autenticación MAC
- Administración del ancho de banda
- Información del usuario y estadísticas de Radius
- Walled Garden
- avisos URLs
- Página de redirección configurable

- Administración MAC
- Soporta atributos de Radius
- Configuración de la interfaz WAN (PPPoE, PPTP)
- Información de concesiones DHCP.
- Funciones inalámbricas
- Seguridad inalámbrica avanzada (WPA, 802.1x)
- Mejor algoritmo de selección de canal
- Selección del código de país
- Filtrado de tráfico inalámbrico a inalámbrico
- Mac Address Spoofing
- Funciones avanzadas de firewall
- Servicio NTP (Network Time Protocol)

1.4 Guía de Instalación del NETKROM NMS

Para instalar el Netkrom NMS en Windows, doble click en el instalador NETKROM_vX_setup.exe y siga las indicaciones. El instalador viene con jre 1.4, por lo tanto usted no tiene que pre instalarlo.

Para instalar el Netkrom NMS en Linux o Mac, descomprima el archivo *NNMSvX_jars.zip* y ejecute la aplicación java –jar NNMSvX.jar desde el directorio actual. JRE (v1.4) debe estar pre instalado.

2. NETKROM NMS

Si su objetivo es desplegar varios access points en un solo sistema, la administración central es recomendada. Incluso si usted planea empezar con una red pequeña, pero espera expandirla en el futuro, un sistema de administración centralizada debe ser considerado. El NETKROM Network Management System (NNMS) suministra una solución de administración segura que cubre las necesidades de la mayoría de los usuarios.

Usando **NNMS** usted puede:

Administrar access points y dispositivos en la red inalámbrica

Configurar nodos de red y otros parámetros

- Cargar y guardar configuraciones de red
- Configurar y ver la topología de red
- Descubrir nodos disponibles
- Analizar el tráfico de red usando el Multi Router Traffic Grapher (MRTG)

2.1 Descripción de la Interfaz NNMS

La interfaz del usuario utiliza los típicos menús desplegables, menús de atajo (click derecho) y paneles con pestañas y sub pestañas dentro de la ventana principal.

Ventana Principal del NNMS

El NETKROM NMS es una interfaz gráfica de usuario que permite y facilita la observación, configuración y monitoreo de su red inalámbrica. La interfaz incluye un típico menú principal, pestañas, información textual y menús de atajo los cuales le permiten navegar por otras ventanas, pestañas y cuadros de diálogo.

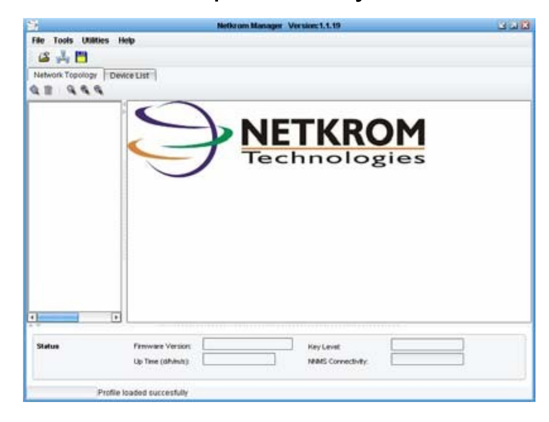


Figura 1. Ventana Principal del NNMS

Menú Principal

El **NETKROM NMS** cuenta con un sistema de 4 menús principales los cuales son: **File**, **Tools**, **Utilities** y **Help**.

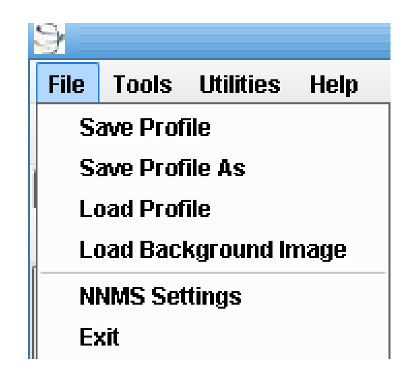


Figura 2. Sistema de Menús Principales del NNMS

Paneles con Pestañas

El cuerpo principal del NNMS muestra información en paneles con pestañas. Cuando el NNMS se inicia la pestaña **Network Topology** está disponible. Esta pestaña contiene información de 3 paneles: **Topology Map**, **Registered Node List** y **Node Status**.



Figure 3. Paneles con Pestañas del NNMS

Menú de Atajos del Nodo

Muchas otras funciones son accesibles vía el menú **Node Shortcut Menu**, el cual incluye los siguientes ítems: **GUI-Node Connectivity Settings, Open Status Window, Advanced Node Configuration, Save Configuration, Unlock, Back Up, FW Upgrade, Reboots, Current Throughput, Wisp Easy Wizard (WEW)** y **Remove.** Desde el menú de atajos del nodo usted puede acceder a pestañas y ventanas usadas en la configuración y monitoreo de la red.

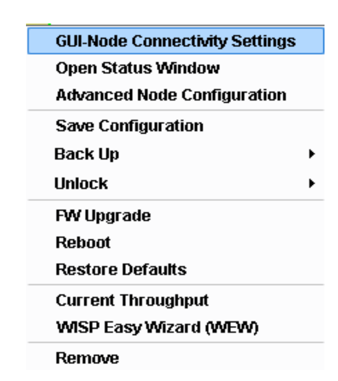


Figura 4. Menú de Atajos del Nodo

2.1.1 Menú Principal del NETKROM NMS

Usando los menús del NNMS usted puede administrar perfiles del sistema, implementar herramientas para descubrir, agregar y ver nodos, ejecutar utilidades y acceder a la información de ayuda. Estos menús principales incluyen:

File

- **Save Profile** – Guarda el perfil actual del NMS
- **Load Profile** – Carga un perfil NMS previamente guardado
- **Load Background Image** – Carga una imagen de fondo (típicamente un mapa) para ser mostrado en el mapa de topología
- **NMS Settings** – Establecer el intervalo de sondeo y los valores de los puertos para el sondeo
- **Exit** – Salir del NNMS

Tools

- **View Topology** – Muestra la pestaña del mapa de la topología
- **Add New Node** – Abre el cuadro de diálogo para insertar un Nuevo nodo
- **License Manager** – Muestra la pestaña del administrador de licencias
- **Discovery Manager** – Abre el cuadro de diálogo de detección automática

Utilities

MRTG – Abre la ventana del MRTG

Help

- **Home Page** – Acceder a la página web de NETKROM
- **About** – Muestra la venta introductoria de NETKROM

2.1.2 Información de los Paneles de la Pestaña Topología de Red

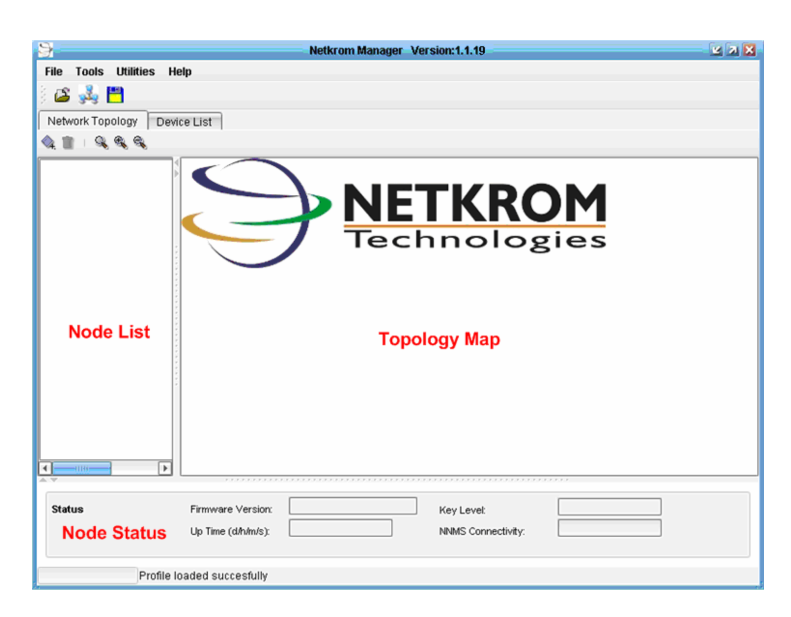


Figura 5. La Ventana del NETKROM NMS

Topology Map

Ubicado en el panel central, el **Topology Map** muestra íconos que representan a los nodos de red e información de conexión describiendo el diseño de la red. También puede mostrar un mapa o imagen como fondo.

Registered Node List

Es el panel de la izquierda, el panel **Registered Node List** muestra todos los nodos registrados de la red.

Node Status

Es el panel de abajo, el panel **Node Status** muestra la siguiente información del nodo seleccionado:

Firmware Version – El número que representa la version del firmware del nodo

- **Up Time** – El tiempo que el nodo ha estado operando
- **Key Level**
- **NNMS Connectivity** – El radio de las respuestas de prueba recibidas satisfactoriamente.

Todos estos paneles pueden ser ajustados de acuerdo a las preferencias del usuario.

2.1.3 Menú de Atajos del Nodo

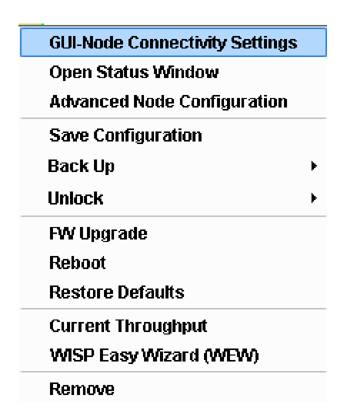


Figura 6. Menú de Atajos del Nodo

GUI-Node Connectivity Settings

La opción **GUI-Node Connectivity Settings** le permite acceder al cuadro de diálogo **Node Connectivity Settings** (Para el nodo seleccionado).

Open Status Window

La opción **Open Status Window** le permite acceder al cuadro de diálogo **Status**, el cual contiene los campos de **FW Version, Key Level, Up Time** y **Host Name**. (Los campos FW Version, Key Level y Up Time también son mostrados en el panel **Node Status** de la pestaña **Topology Map**.)

Advanced Node Configuration

La opción **Advanced Node Configuration** le permite recuperar información desde el nodo seleccionado. Un Nuevo panel es mostrado conteniendo una pestaña principal (**Advanced Configuration of node: [Nombre del Nodo].** Debajo de esta pestaña 3 sub-pestañas son mostradas: **Configuration, Statistics** y **System Properties.** Cada una de estas pestañas contiene varias sub pestañas usadas en el proceso de configuración.

Save Configuration

La opción **Save Configuration** le permite guardar permanentemente la configuración actual del nodo.

> ***Nota:*** *Después de que el nodo es configurado, los parámetros configurados son almacenados en la RAM (memoria volátil). Si el nodo se apaga, la configuración se perderá a menos que usted guarde la configuración en la memoria permanente del nodo.*

Back Up

La opción **Back Up** le permite hacer un backup y restaurar la configuración para un nodo seleccionado.

FW Upgrade

La opción **FW Upgrade** le permite acceder al cuadro de diálogo **Select**, desde el cual usted puede seleccionar el archivo imagen del firmware que va ser cargado dentro del nodo.

Reboot

La opción **Reboot** le permite reiniciar el nodo.

Current Throughput

La opción **Current Throughput** le permite mostrar un gráfico en tiempo real del tráfico que se transmite y recibe por el nodo.

WISP Easy Wizard (WEW)

La opción **WISP Easy Wizard (WEW)** le permite iniciar el wizard el cual suministra una manera fácil y conveniente de instalar y configurar nodos inalámbricos. (Vea el capítulo 16 para más detalles)

Remove

La opción **Remove** le permite eliminar el nodo seleccionado del **Topology Map** y **Registered Node List**.

2.2 Introducción al NNMS

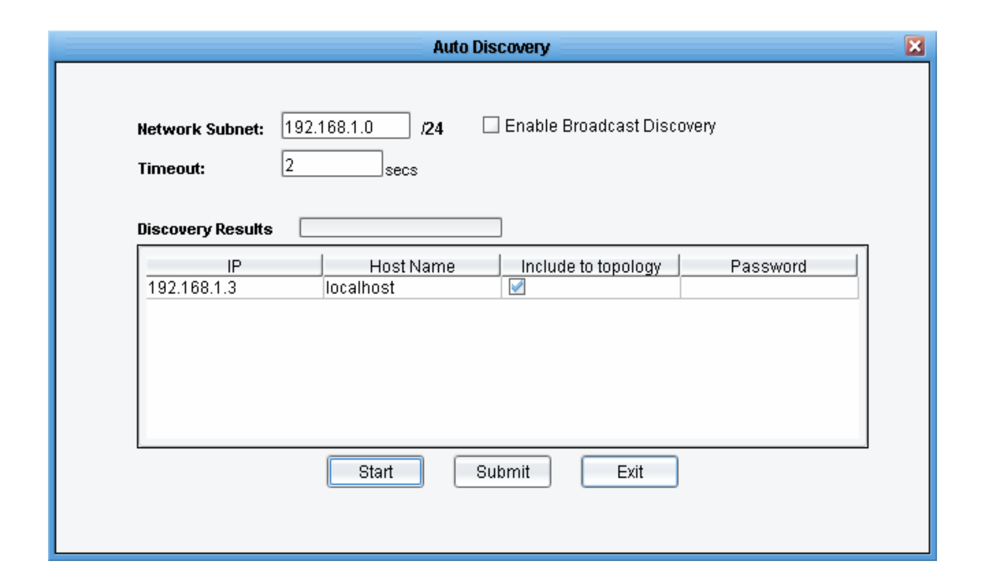
Empezando con los menús y ventanas mencionados arriba, usted puede descubrir e insertar nodos, mostrar mapas y gráficos de su red inalámbrica, guardar y cargar perfiles y acceder a las múltiples pestañas usadas para las configuraciones avanzadas de los nodos.

2.2.1 Descubriendo Nodos

Discovery Manager le permite descubrir nodos e insertarlos dentro del **Topology Map.** Un protocolo de sondeo es utilizado para detector los nodos Netkrom en la subred especificada. Los nodos descubiertos son mostrados en un formato tabular.

Para usar el **Discovery Manager**:

En el menú **Tools**, seleccione **Discovery Manager**. El cuadro de diálogo de **Discovery** aparecerá.



Cuadro de Diálogo del Auto Discovery

Network Subnet

En el campo **Network Subnet**, escriba la dirección de la subred. (NNMS detectará los nodos que estén en la misma subred)

Enable Broadcast Discovery

Seleccione la casilla **Enable Broadcast Discovery**. (NNMS usa un mensaje broadcast UDP en la subred)

Timeout

En el campo **Timeout**, escriba el valor del tiempo de espera para el sondeo (por defecto: 10 segundos)

Discovery Results

Click en **Start** para iniciar un sondeo de descubrimiento. La barra gráfica **Discovery Results** muestra el progreso del sondeo. Cuando el sondeo se complete, la tabla muestra el **IP Address**, **Host Name** y **Password** (si se usa) de los nodos descubiertos. La casilla debajo de **Include to Topology** está automáticamente seleccionada.

Include to Topology

Para mostrar un nodo en el **Topology Map**, marque la casilla **Include to Topology**.

Submit

Click en el botón **Submit** para insertar los nodos dentro del **Topology Map.**

Cancel

Click en el botón **Cancel** para salir del cuadro de diálogo **Auto Discovery**.

Los íconos para cada nodo deberían ser visibles en el **Topology Map**, etiquetado con el nombre del nodo. Si dos nodos tienen el mismo nombre, el NNMS etiquetará a uno con el nombre y al otro con su dirección IP. (La etiqueta puede ser cambiada a un alias usando el cuadro de diálogo **GUI-Node Connectivity Settings**, accesible desde el **Node Shortcut Menu.)**

2.2.2 Configurando un Nuevo Nodo

Los nodos de red pueden ser configurados manualmente usando el cuadro de diálogo **Insert New Node**.

1. Use cualquier de los siguientes tres métodos para configurar un nuevo nodo

- Click en cualquier lugar del panel de topología, luego click en el botón **Insert new node** que aparece o click en el ícono O en el menú **Tools,** click en **Add New Node**. El cuadro de diálogo **Insert New Node** aparece.

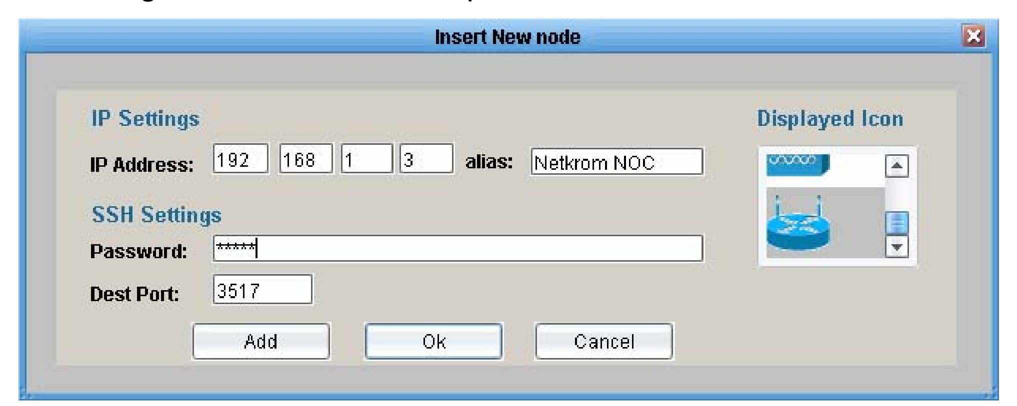
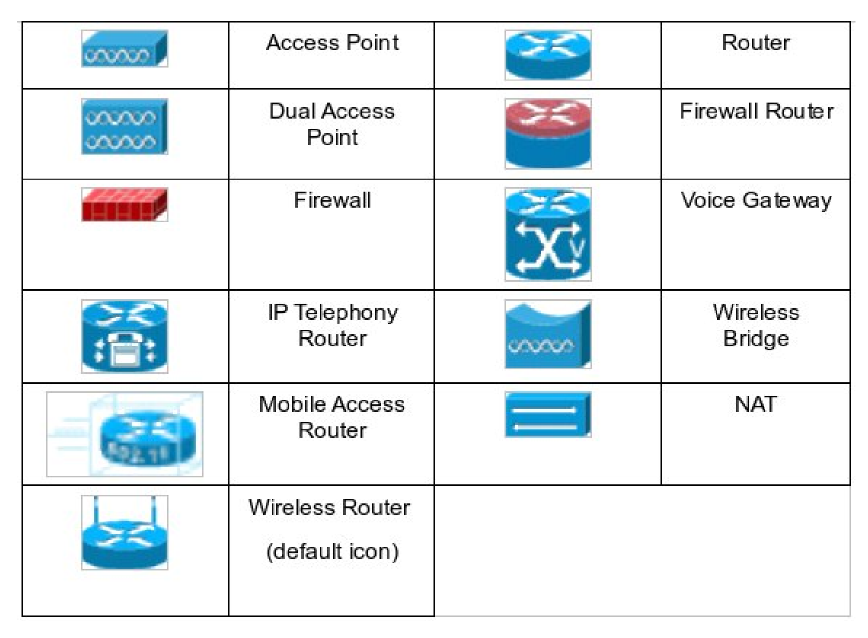


Figura 7. Cuadro de diálogo de insertar un Nuevo nodo

2. Escriba la dirección IP en **IP address**, el alias en **Alias** (opcional) y la contraseña en **Password**. (Típicamente un Nuevo nodo tiene la contraseña por defecto admin*)*

3. Seleccione un ícono en el panel **Displayed Icon** (opcional) para representar el nodo.



	Access Point		Router
	Dual Access Point		Firewall Router
	Firewall		Voice Gateway
	IP Telephony Router		Wireless Bridge
	Mobile Access Router		NAT
	Wireless Router (default icon)		

Figura 8. Lista de íconos disponibles

> ***Nota:*** *Aunque es opcional, agregar un* ***Álias*** *y un* ***Ícono*** *suministra una representación visual mejorada de los nodos. Esto es muy útil cuando trabaje con redes medianas y grandes.*

4. Click en el botón **Add**. El ícono aparecerá en el panel de topología. Toda la topología es actualizada con la inserción de nueva información.

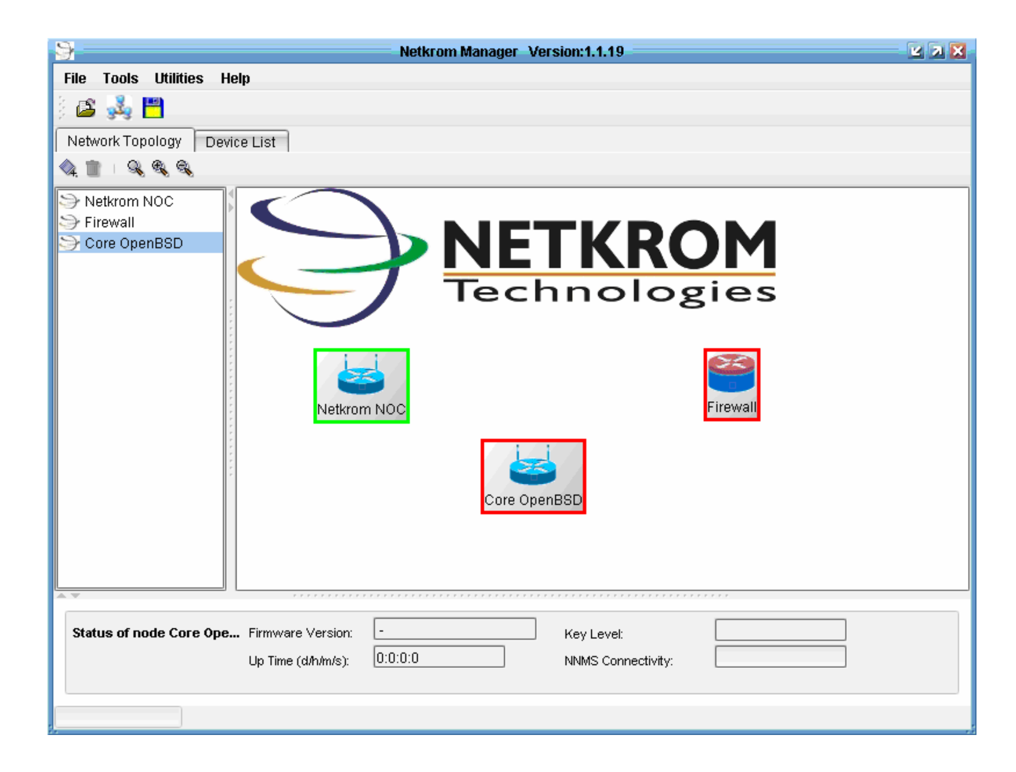


Figura 9. Inserción de un nodo

Si el Nuevo nodo insertado ha respondido satisfactoriamente, una línea verde aparecerá alrededor del ícono, en caso contrario una línea roja indicará que el nodo no está respondiendo como se muestra en la figura de la derecha.

localhost

2.2.3 Moviendo y Cambiando de Tamaño a los Íconos

- Para mover el ícono de un nodo, arrástrelo a la ubicación deseada del panel. Para cambiar de tamaño del ícono de un nodo, seleccione el ícono, y luego arrastre una de sus esquinas.

2.2.4 Agregando Imágenes como Fondo

El **Topology Map** puede ser mejorado cargando una imagen como fondo para indicar la ubicación geográfica de los nodos. Para agregar una imagen de fondo:

- En el menú **File**, click en **Load Background Image**. El cuadro de diálogo **Load Background Image** aparece.

- Busque la imagen que usted desea cargar, selecciónelo y haga click en el botón **Load Background Image**.

Nota: *.Solo los formatos gif o .jpg pueden ser usados como fondos*

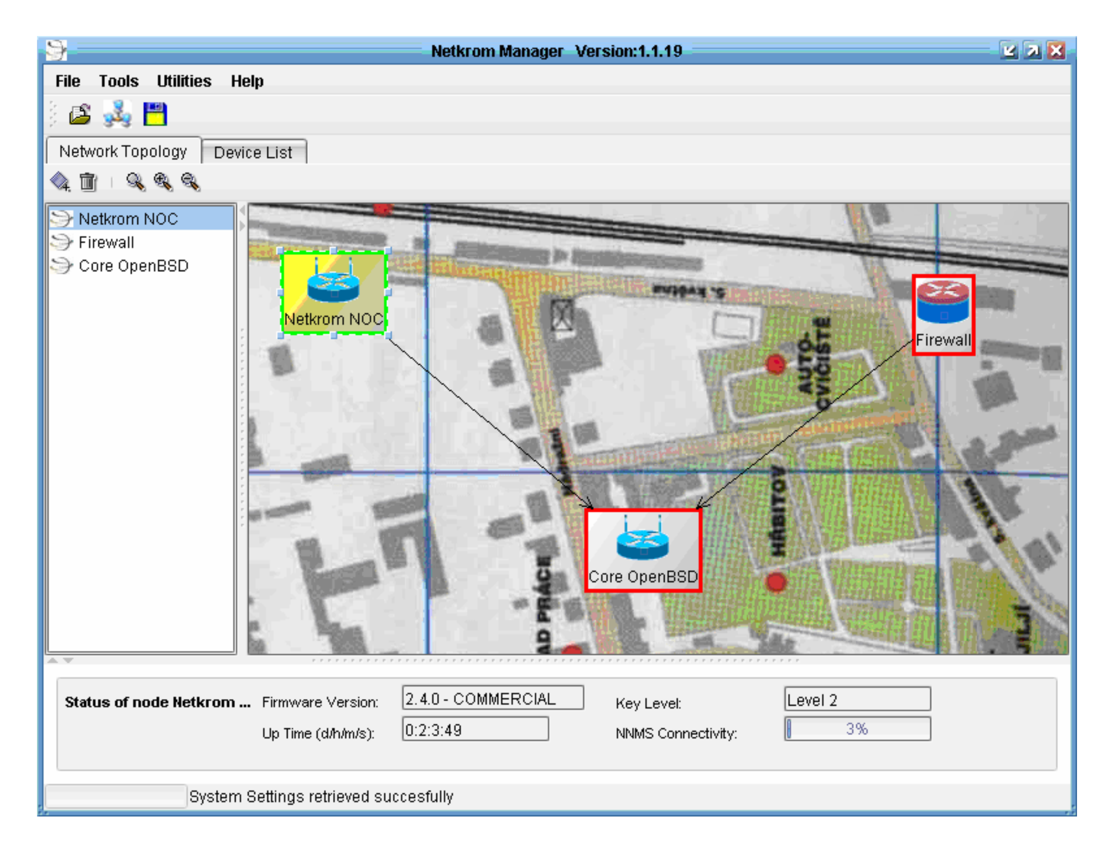
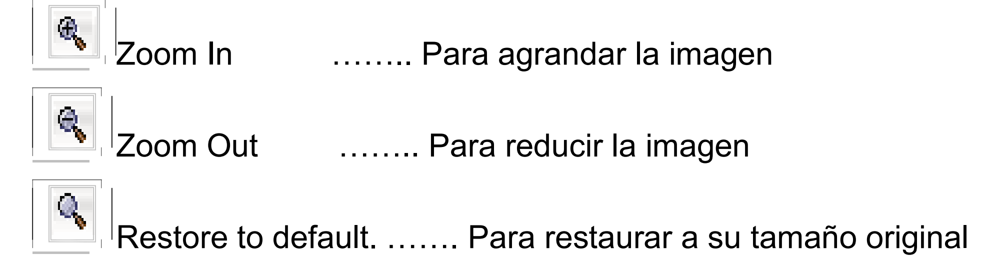


Figura 10. Mapa de topología personalizado

- Ajuste el nivel de aumento del fondo usando los botones zoom ubicados arriba de **Registered Node List**:

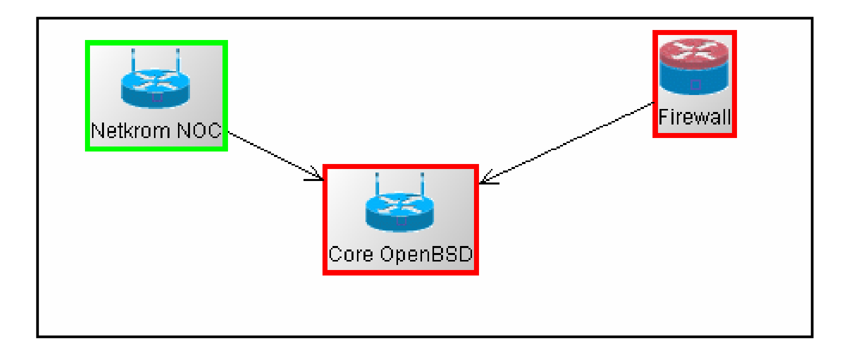


Zoom In .... Para agrandar la imagen

Zoom Out .... Para reducir la imagen

Restore to default. .... Para restaurar a su tamaño original

- Cree flechas indicando una conexión entre nodos hacienda click en el centro del nodo de origen (una mano como cursor aparecerá), y arrástrelo hasta el centro del nodo de destino. Una flecha aparecerá entre los nodos.



Nodos de red mostrando dos conexiones

2.2.5 Guardando y Cargando Perfiles

1. Para guardar un perfil, en el menú **File**, click en **Save Profile**.

2. Para cargar un perfil, en el menú **File**, click en **Load Profile**.

2.2.6 Usando el Menú de Atajos del Nodo

Usted puede administrar y configurar una variedad de parámetros de operación de los nodos de red usando el menú **Node Shortcut Menu,** el cual puede ser accedido usando los siguientes métodos:

Doble click en el nombre de un nodo de la lista **Node List** o

- Click derecho en un nodo del mapa de topología

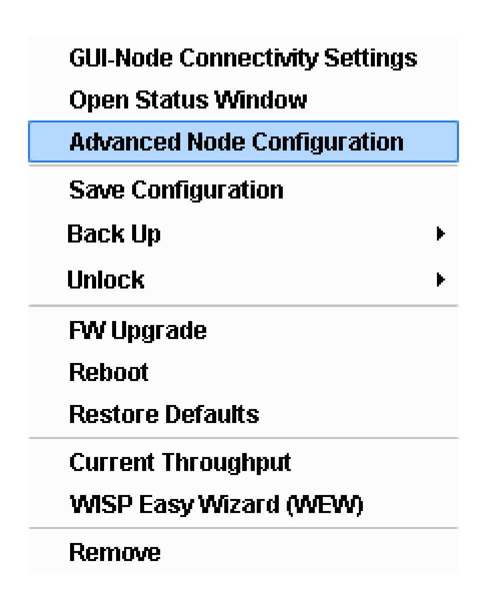


Figura 11. Menú de atajos del nodo

Gui-Node Connectivity Settings

Click en esta opción para mostrar el cuadro de diálogo del **Node Connectivity Setting**. Este cuadro contiene la dirección PI y alias asignados al ícono seleccionado. Si el alias no ha sido asignado, el campo alias contendrá el nombre del nodo.

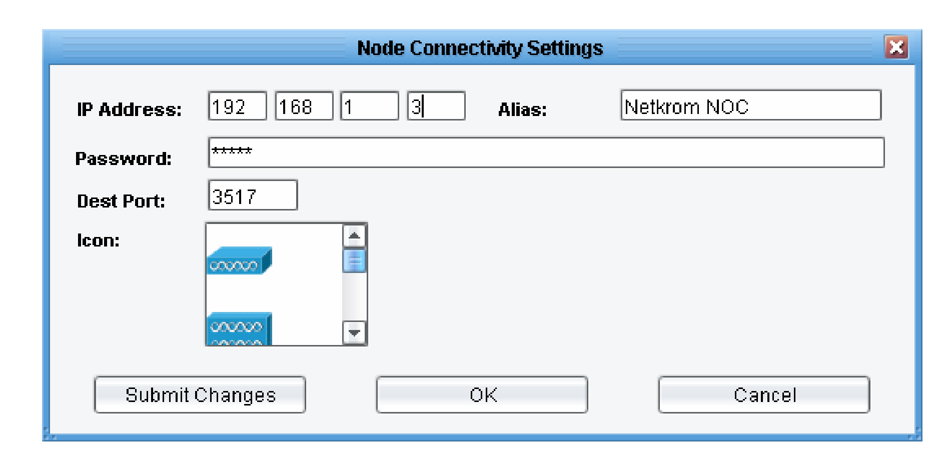


Figura 12. Cuadro de diálogo de la configuración de conectividad del nodo

IP Address

Cuando el NETKROM NMS escanea la red, busca la dirección IP que se ha ingresado. Si la conexión es satisfactoria, una línea verde aparece alrededor del ícono pero si la conexión no es satisfactoria, una línea roja aparece alrededor del ícono.

Dirección IP por defecto: 192.168.1.3

Alias

Para cambiar el **Alias**, escriba el nuevo alias dentro del cuadro de texto Alias.

Password

Escriba la contraseña (Por defecto: *admin)* dentro del campo **Password**. (Este paso es obligatorio para accede al **Advanced Node Configuration** descrito más adelante en esta sección.)

Node Icon

Para cambiar el ícono del nodo, seleccione un ícono de la lista.

Submit Changes

Click en el botón **Submit Changes** para agregar el nodo al mapa de topología y mantener abierto el cuadro de diálogo.

OK

Click en **OK** para agregar el nodo y salir del cuadro de diálogo

__NOTA__: La dirección IP y contraseña será usado cuando el NNMS escanea la red. Cambiar la dirección IP del ícono no cambia la dirección IP del nodo. Si la dirección IP del ícono se cambia a una dirección que no está presente en la red, el borde del ícono se volverá rojo indicando que ninguna conexión se ha hecho.

Open Status Window

Click en esta opción para acceder al cuadro de diálogo de **Status**, el cual contiene los campos **FW (Firmware) Version, Key Level, Up Time** y **Host Name**. (Los campos FW Version, Key Level y Up Time también son mostrados en el panel **Node Status** de la pestaña **Topology Map**.)

- El campo **FW Version** contiene la version del firmware del nodo seleccionado.
- El campo **Key Level** debería mostrar Level 2.
- **Up Time** – El tiempo que el nodo ha estado operando.
- **Host Name** – El nombre del nodo seleccionado.

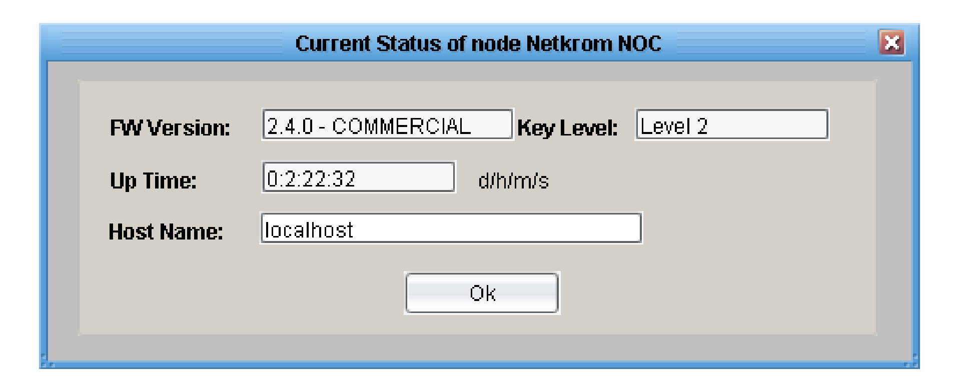


Figura 13. Cuadro de diálogo de Status

Advanced Node Configuration

Click en esta opción para recuperar la información del nodo seleccionado y abrir la pestaña **Advanced Configuration of Node.**

__NOTA:__ Para acceder a la pestaña Advanced Node Configuration usted primero debe acceder a Node Connectivity Settings vía el menú Node Shortcut e ingresar el password, luego click en OK o Submit.

La pestaña **Advanced Configuration of Node** contiene tres sub pestañas:
Configuration, Statistics y **System Properties.**



Figura 14. Pestaña Advanced Node Configuration con sus tres sub pestañas

Cada pestaña contiene varias pestañas adicionales. El mapa de abajo muestra la jerarquía de la pestaña Advanced Node Configuration. La tabla muestra los capítulos donde son descritos y explicados.

Pestaña	**Capítulo**
Network	3, 4
VLAN	3
Wireless	5
Firewall	6
NAT	6
DHCP	7
WAN	8
Bandwidth Manager	9
HotSpot	10
Services	11
Statistics	12

Figura 15. Lista de pestañas y capítulos

Jerarquía de la Pestaña Advanced Node Configuration

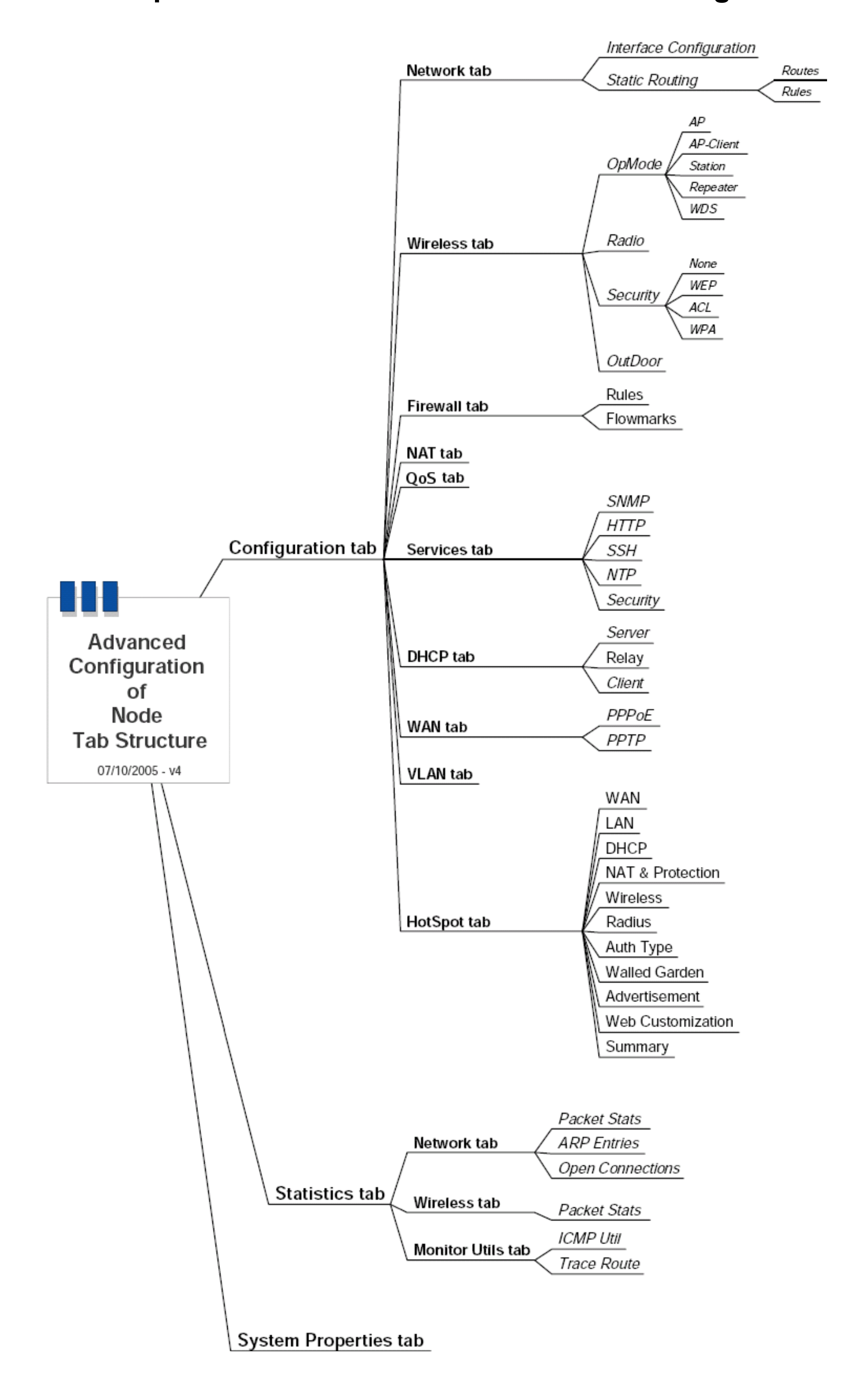


Figura 16. Mapa de la Pestaña Advanced Configuration y sus sub pestañas

Save Configuration

Click en esta opción para guardar permanentemente la configuración del nodo actual.

> ***Nota:*** *Después de que el nodo es configurado, los parámetros de configuración son almacenados en la memoria RAM (memoria volátil). Si el nodo se apaga, la configuración en la memoria permanente del nodo.*

Back Up

Click en esta opción y seleccione:

- **Retrieve Configuration** para recuperar la última configuración guardada

Restore Configuration para restaurar la configuración de un nodo desde un archivo

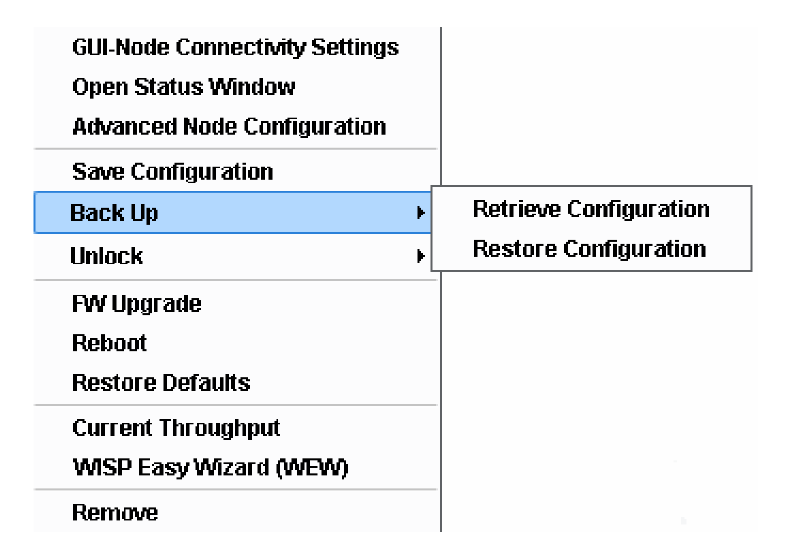


Figura 17. Opciones de Back Up

FW Upgrade

Click en esta opción para acceder al cuadro de diálogo de **Select**, desde el cual usted puede seleccionar el firmware que va ser cargado en el nodo.

Reboot

Click en esta opción para reiniciar el nodo. Un cuadro de diálogo de alerta **Alert** aparecerá con la siguiente pregunta: **Should system save its configuration before reboot** que significa si usted desea guardar la configuración antes de reiniciar**.** Click en **Yes** si usted quiere guardar la configuración.

Current Throughput

Click en esta opción para mostrar un gráfico en tiempo real del tráfico recibido y transmitido del nodo.

WISP Easy Wizard (WEW)

Click en esta opción para empezar el Wizard el cual suministra una manera fácil y sencilla de instalar nuevos nodos. (Vea el capítulo 16 para más detalles)

Remove

Click en esta opción para eliminar el nodo seleccionado del mapa de tipología y de la lista de nodos registrados.

3. Configuraciones IP

Esta sección describe los parámetros y configuraciones IP de los nodos.

Para configurar los parámetros IP, seleccione la pestaña **Interface Configuration [Configuración de Interfaz]**, ubicado debajo de **Advanced Configuration of Node [Configuración Avanzada del Nodo], Configuration [Configuración],** y luego **Network [Red]**.

La pestaña **Interface Configuration [Configuración de Interfaz]** contiene 4 paneles:

- **Árbol de Interfaces** (Panel de la izquierda)
- **Configuración IP Básica** (Panel de arriba)
- **Configuraciones Globales** (Panel del centro)
- **Comandos de Acción Especial** (Panel de abajo)

Además dos botones están ubicados al costado de la pestaña IP Configuration:

- **Refresh [Actualizar]** – Click en este botón para actualizar la configurar del nodo seleccionado
- **Submit [Enviar]** – Click en este botón para cargar la configuración al nodo.

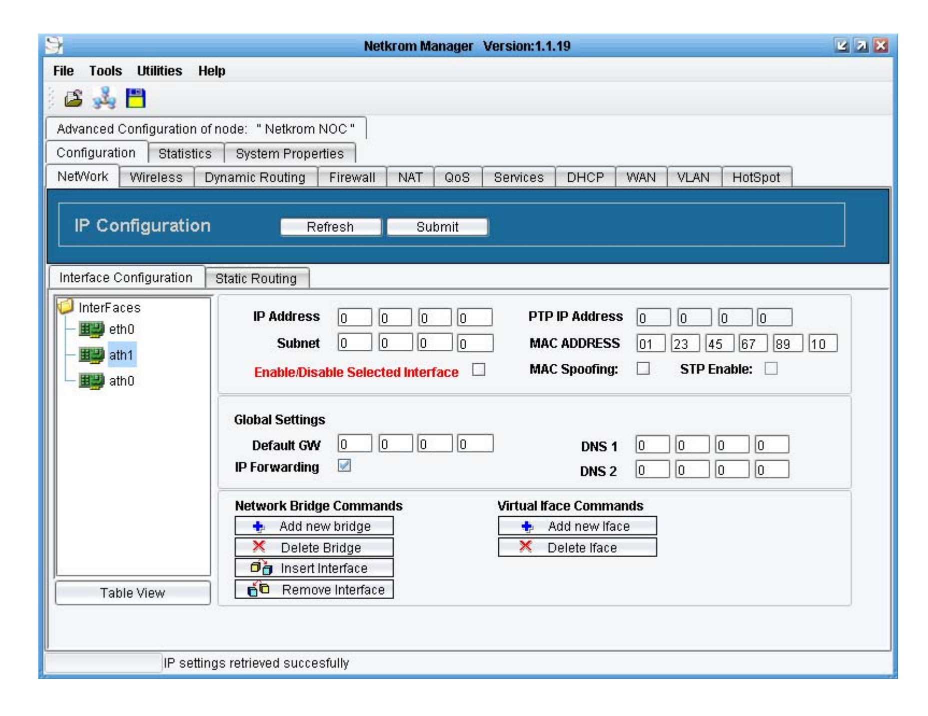


Figura 18. Pestaña Network Configuration

3.1 Usando el Árbol de Interfaces

El panel izquierdo de la pestaña **IP Configuration [Configuración IP]** contiene el árbol de interfaces, el cual es una representación de las interfaces disponibles del nodo. Este panel puede ser expandido o reducido. Cuando una interfaz es seleccionada, los campos de los otros paneles muestran los parámetros asociados a la interfaz seleccionada.

3.2 Configuración IP Básica

El panel de arriba de la pestaña **IP Configuration [Configuración IP]** contiene varios campos para su configuración.

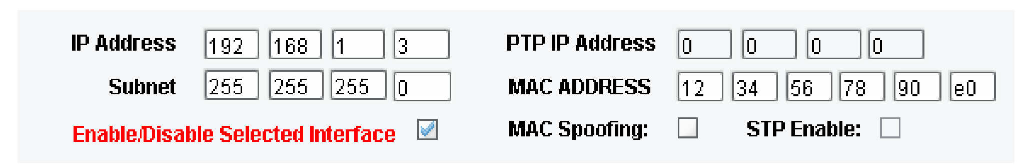


Figura 19. Configuración de Parámetros Básicos IP

3.2.1 IP Address [Dirección IP]

Este campo contiene la dirección IP de la interfaz del nodo seleccionado. Para cambiar la dirección IP de la interfaz, escriba la nueva dirección dentro del campo y luego haga click en el botón **Submit [Enviar]**.

3.2.2 Subnet [Máscara de Subred]

Este campo contiene la máscara de subred de la interfaz seleccionada. Para cambiar la máscara de subred de la interfaz, escriba la nueva máscara de subred dentro del campo y luego haga click en el botón **Submit [Enviar]**.

3.2.3 Enable/Disable Selected Interface [Habilitar/Deshabilitar Interfaz Seleccionada]

Esta casilla sirve para habilitar y deshabilitar la interfaz seleccionada. Cuando está marcada indica que la interfaz está habilitada, por el contrario cuando no está marcada indica que la interfaz está deshabilitada.

3.2.4 PTP IP Address [Dirección IP PTP]

Si hay una conexión PPP (desde un cliente PPPoE o un cliente PPTP), la dirección IP del punto remoto se muestra en el campo **PTP IP Address [Dirección IP PTP].** De otra manera este campo está en blanco. Este campo es de solo lectura es decir no se puede cambiar.

3.2.5 MAC Address [Dirección MAC]

Este campo muestra la dirección MAC de la interfaz seleccionada en formato hexadecimal. Si se desea cambiar la dirección MAC de la interfaz debe habilitar el **MAC Spoofing [Suplantación de MAC]**.

3.2.6 MAC Spoofing [Suplantación de MAC]

Habilite esta casilla para cambiar la dirección MAC, esta opción solo se puede habilitar para las interfaces físicas y no para las virtuales.

3.2.7 STP Enable [Habilitar STP]

Este casilla sirve para habilitar el protocolo spanning tree STP.

> ***Nota:*** *El protocolo Spanning Tree Protocol (STP) elimina los bucles de capa 2 en la red mediante el bloqueo y habilitación de interfaces.*

3.3 Configuración IP de Parámetros Globales

El panel central de la pestaña **IP Configuration [Configuración IP]** contiene los parámetros de configuración global**.**
Estos campos se aplican a todas las interfaces.

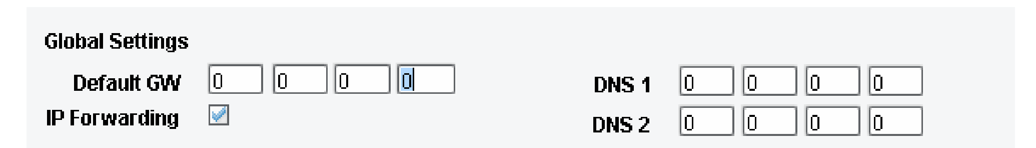


Figura 20. Configuración IP de Parámetros Globales

3.3.1 Default Gateway [Puerta de Enlace Predeterminada]

Todo paquete IP con destino desconocido será enviado a la dirección IP de la puerta de enlace predeterminada. Puede ser configurado manualmente ingresando la dirección IP y también puede ser configurado dinámicamente desde un DHCP, PPPoE o PPTP.

3.3.2 IP Forwarding [Reenvío IP]

Permite que todo el tráfico fluya entre las interfaces incluso si están en diferentes subredes. Marque la casilla para permitir el envío de paquetes de una subred a otra.

3.3.3 DNS1 y DNS2

Usted puede configurar la dirección del DNS1 y DNS2 manualmente o dinámicamente desde un servidor DHCP, PPPoE o PPPTP. El DNS le permitirá resolver los nombres de dominio.

3.4 Usando los Comandos de Acción Especial

El panel de abajo de la pestaña **IP Configuration [Configuración IP]** contiene comandos de acciones especiales usados para crear y administrar bridges e interfaces virtuales.

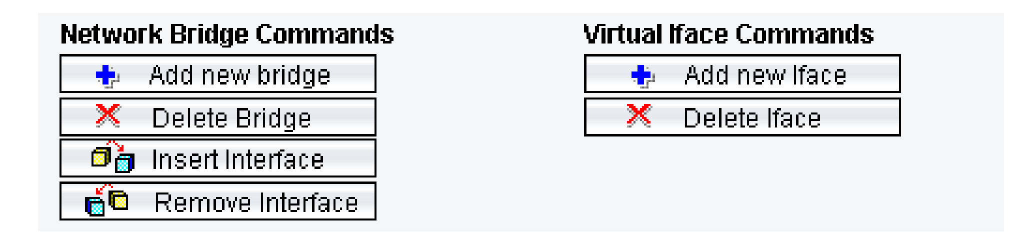


Figura 21. Comandos de acción especial

3.4.1 Network Bridge Commands [Comandos Bridge]

Un bridge es un dispositivo de interconexión LAN que opera en la capa de enlace de datos (Capa 2) del modelo de referencia OSI. Puede ser usado para unir dos segmentos LAN (A, B), construyendo una LAN más grande. Un bridge es capaz de filtrar el tráfico que pasa entre las dos LANs y puede mejorar la política de seguridad separando diferentes grupos de trabajo ubicados en cada una de las LANs. Los Bridges fueron por primera vez especificados en el IEEE 802.1D (1990) y después por ISO (en 1993).

Agregar un nuevo bridge

Para crear un Nuevo bridge:

1. Click en el botón **Add new bridge [Agregar un nuevo bridge]**. El cuadro de diálogo de **Insert New Bridge [Insertar un nuevo bridge]** aparecerá.

2. Escriba el nombre del bridge en el cuadro, luego click en el botón **Submit [Enviar]**. El nombre de bridge aparece en **Network Interfaces Tree [Árbol de interfaces]**.

Nota: *El nombre del bridge debe empezar con las letras "br". No hay limitación en el resto del nombre.*

Eliminar un Bridge

Para eliminar un bridge:

1. Seleccione el bridge en el panel **Network Interfaces Tree [Árbol de interfaces]**
2. Click en el botón **Delete Bridge [Eliminar Bridge]** en el panel **Network Bridge Commands [Comandos Bridge]**

Insertar interfaz

Para insertar una interfaz a un bridge:

1. En el panel **Network Interfaces Tree [Árbol de interfaces],** seleccione la interfaz a insertar.

2. Click en el botón **Insert Interface [Insertar Interfaz]**. El cuadro de diálogo de insertar interfaz aparece.

3. En la lista **Select Bridge [Seleccionar Bridge]**, seleccione el bridge deseado.

4. Click en **Submit [Enviar]**. El árbol de interfaces es reordenado para mostrar la interfaz dentro del bridge al cual pertenece.

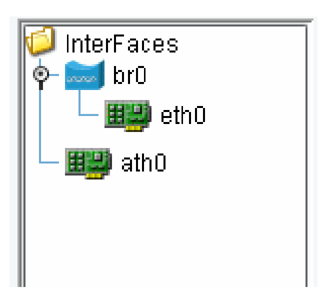


Figura 22. Insertando una interfaz a un bridge

Eliminar Interfaz

1. Seleccione la interfaz del árbol de interfaces.

2. Click en el botón **Remove Interface [Eliminar interfaz]**.

3.4.2 Virtual Interface Commands [Comandos de Interfaz Virtual]

Desde el panel de comandos de acción especial usted puede crear interfaces virtuales las cuales no están asociadas con el hardware. Las interfaces virtuales le permiten asociar más de una dirección IP con un sistema. Un uso típico de esta técnica es el soporte de múltiples Webs. Por ejemplo, si http://www.examplesite.com fuera asignado a 222.33.44.55, las interfaces virtuales 222.33.44.56 y 222.33.44.57 podrían ser asignadas a www.examplesite.net y www.examplesite.org. Los tres sitios web podrían existir en el mismo sistema sin ningún conflicto.

Las interfaces virtuales también permiten que un sistema se comunique con más de un espacio de direcciones de red. Por ejemplo, las interfaces virtuales le permiten temporalmente re numerar una red de un espacio de direcciones de red enmascarados a una subred privada (10.0.0.0). Durante la transición, todos los servidores pueden ser asignados a una dirección virtual habilitándolos para comunicarse con clientes en ambos en el antiguo y nuevo espacio de direcciones de red. Externamente, las interfaces virtuales aparecen como si fueran interfaces físicas.

Agregar una nueva interfaz virtual

Para insertar una nueva interfaz virtual en asociación con una interfaz física:

1. Seleccione la interfaz física desde el panel **Network Interfaces Tree [Árbol de interfaces].**

2. Click en el botón **Add new Interface [Agregar nueva interfaz]**. La interfaz virtual aparece en el árbol y es automáticamente nombrado con un prefijo que concuerda con la interfaz física y un sufijo que es un número dentro de corchetes.

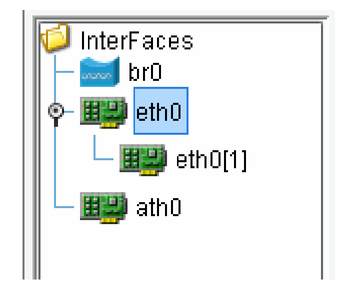


Figura 23. Insertando una interfaz virtual

Eliminar una interfaz virtual

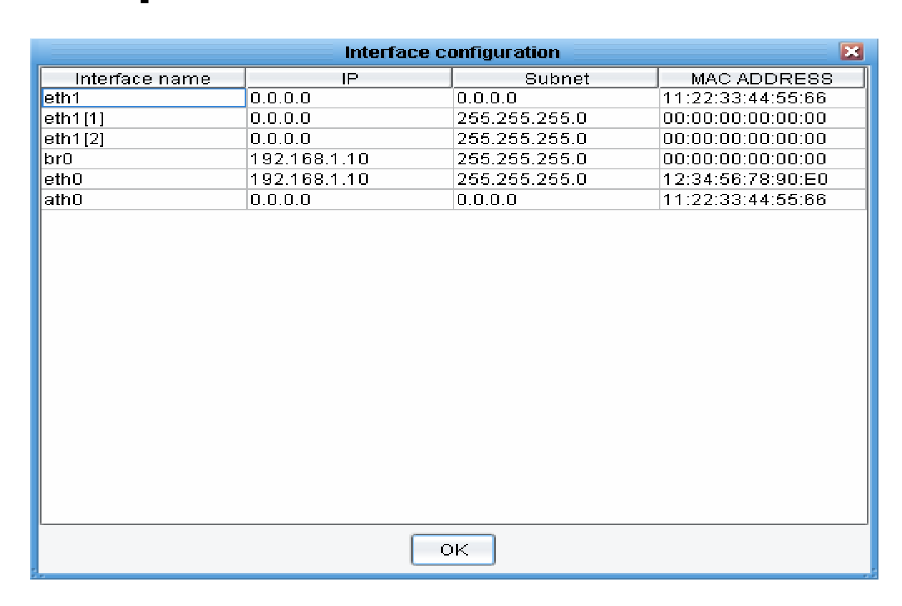
Para eliminar una interfaz virtual:

1. Seleccione la interfaz virtual desde el panel **Network Interfaces Tree [Árbol de interfaces]**

2. Click en el botón **Delete Interface [Eliminar interfaz]**

3.5 Using Table View [Usando Ver Tabla]

La opción **Table View [Ver Tabla]** es una característica que mejora el control de las configuraciones IP de las interfaces. Esta característica le permite buscar y editar configuraciones básicas de todas las interfaces. Para accede a esta opción, click en el botón **Table View [Ver Tabla]** ubicado debajo del panel **Network Interface Tree [Árbol de interfaces]**. El cuadro de diálogo de **Interface Configuration [Configuración de interfaz].**



Interface name	IP	Subnet	MAC ADDRESS
eth1	0.0.0.0	0.0.0.0	11:22:33:44:55:66
eth1 [1]	0.0.0.0	255.255.255.0	00:00:00:00:00:00
eth1 [2]	0.0.0.0	255.255.255.0	00:00:00:00:00:00
br0	192.168.1.10	255.255.255.0	00:00:00:00:00:00
eth0	192.168.1.10	255.255.255.0	12:34:56:78:90:E0
ath0	0.0.0.0	0.0.0.0	11:22:33:44:55:66

Figura 24. Ver Tabla de Interfaces

3.6 Configuración de VLANs

Una LAN virtual (VLAN) es un grupo de dispositivos en una o más LANs que son configuradas para que puedan comunicarse como si estuvieran en la misma red, cuando en realidad están ubicadas en un número de segmento de LAN diferente. Ya que las VLANs están basadas en lógica y no en conexiones físicas ofrecen una Buena administración, control de ancho de banda, etc. La especificación IEEE 802.1Q establece un método estándar para las tramas de Ethernet.

El estándar IEEE 802.1Q define la operación de VLAN en bridges que permiten la definición, operación y administración de topologías de VLAN dentro de una infraestructura de LAN con bridges. El estándar 802.1Q pretende abordar el problema de cómo dividir redes grandes en partes más pequeñas para que el tráfico broadcast y multicast no afecte el ancho de banda. El estándar también ayuda a suministrar un mayor nivel de seguridad entre segmentos de redes internas.

Para que el dispositivo cumpla con el estándar 802.1Q, una o más interfaces con VLAN deben ser creadas con las etiquetas apropiadas. Esto se puede conseguir en la pestaña **VLAN** del NETKROM NMS. Las interfaces con VLAN pueden ser agregadas, eliminadas y administradas desde esta pestaña.

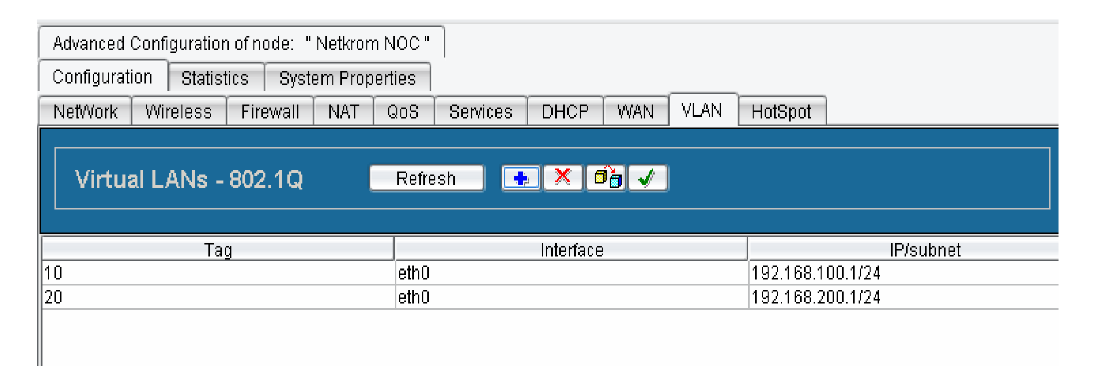


Figura 25. Pestaña VLAN

3.6.1 Agregando Interfaces VLAN

1. En la pestaña **VLAN**, click en el botón . El cuadro de diálogo de **Create a new VLAN [Crear una nueva VLAN]** aparece. Este cuadro de diálogo contiene los campos principales para configurar la interfaz VLAN. El campo **VLAN Tag ID [ID de la Etiqueta de VLAN]** automáticamente genera un identificador único para la VLAN de acuerdo a 802.1Q.

2. Seleccione la interfaz física o bridge de la lista desplegable.

3. Escriba la dirección IP y máscara de subred en los campos **IP Address [Dirección IP]/Subnet Mask [Máscara de subred]**. Estos campos son necesarios para rutear los paquetes correctamente etiquetados. Si hay necesidad de poner paquetes no etiquetados (no compatible con 802.1Q), configure la interfaz física específica y cualquier interfaz virtual con la dirección IP de cero.

4. Click en **Submit [Enviar]** para completar el proceso. El número de la etiqueta de la interfaz, nombre de la interfaz y dirección IP/máscara aparecerá en la lista Virtual LAN.

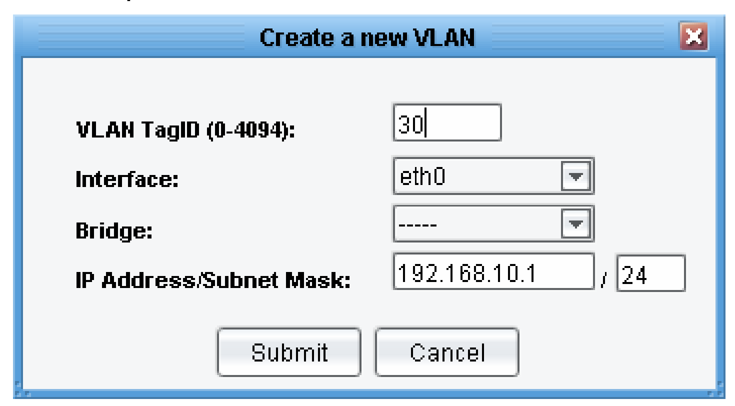


Figura 26. Creando una nueva VLAN

3.6.2 Eliminando interfaces VLAN

Para eliminar una interfaz VLAN, en la lista de VLAN, seleccione la interfaz para ser eliminada. Click en el botón . La información de VLAN desaparecerá de la lista.

3.6.3 Modificando interfaces VLAN

Para modificar la configuración de una interfaz VLAN, seleccione la interfaz y haga click en el botón . El cuadro de diálogo de **Create a new VLAN [Crear una nueva VLAN]** aparece. La configuración de la interfaz se muestra en los campos.

Modifique lo que cree conveniente y luego haga click en el botón **Submit [Enviar]**. La nueva configuración aparece luego en la lista de interfaz de VLAN.

3.6.4 Cargando las interfaces VLAN

Para enviar la configuración al nodo, click en el botón .

4. Ruteo Estático IP

El ruteo estático es el método manual de configurar el enrutamiento. Un administrador ingresa rutas dentro del dispositivo usando comandos de configuración. Este método tiene la ventaja de ser simple de configurar. Es útil en la administración de pequeñas redes pero se vuelve incómodo en redes grandes. NETKROM NMS suministra herramientas de administración para manipular cualquiera de las tablas de ruteo y reglas de configuración.

Para configurar el enrutamiento estático IP, seleccione la pestaña **Static Routing** [Enrutamiento Estático], ubicado debajo de las pestañas **Advanced Configuration of Node [Configuración avanzada del nodo], Configuration [Configuración], Network [Red]**. En la pestaña **Static Routing [Enrutamiento Estático]** usted puede seleccionar la pestaña **Routes [Rutas]** o la pestaña **Rules [Reglas]**.

Vea la página 32 para ver un diagrama de la pestaña Advanced Configuration [Configuración Avanzada] y sus sub pestañas.

En la pestaña **Routes [Rutas]** usted puede:

- Agregar, eliminar y seleccionar tablas de ruteo
- Agregar, eliminar, modificar y priorizar rutas

En la pestaña **Rules [Reglas]** usted puede:

- Agregar, eliminar y seleccionar reglas.

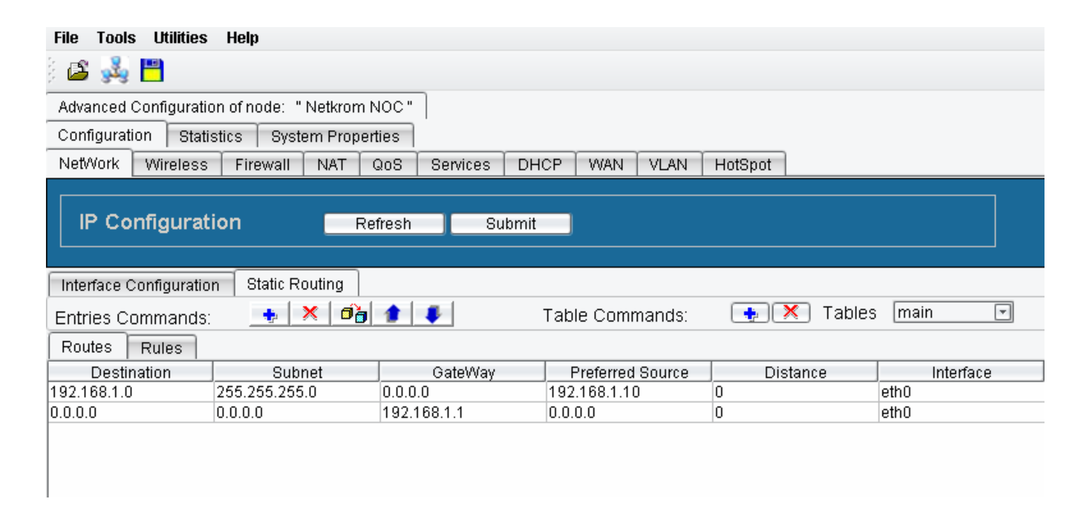
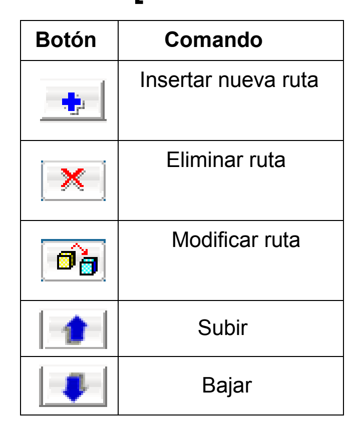


Figura 27. Manejo de la tabla de ruteo

La barra de la parte superior de la pestaña **Static Routing [Enrutamiento Estático]** contiene las siguientes opciones:

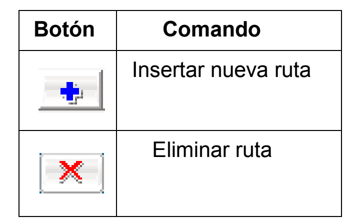
- **Entries Commands [Comandos de Entrada]**



Botón	Comando
	Insertar nueva ruta
	Eliminar ruta
	Modificar ruta
	Subir
	Bajar

Figura 28. Comandos de Entrada

- **Table Commands [Comandos de Tabla]**



Botón	Comando
	Insertar nueva ruta
	Eliminar ruta

Figura 29. Comandos de Tabla

- **Tables [Tablas]**

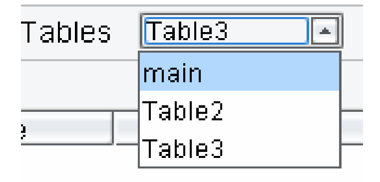


Figura 30. Lista desplegable de las tablas de enrutamiento

4.1 Configurando Tablas de Enrutamiento

NETKROM suministra un sistema múltiple de tablas de enrutamiento con una infraestructura flexible y la habilidad de implementar políticas de enrutamiento. Además de las tablas de enrutamiento local y principal, NETKROM soporta hasta 252 tablas de enrutamiento.

4.1.1 Agregando una nueva tabla de enrutamiento

Para crear una nueva tabla de enrutamiento que esté integrado en el sistema múltiple de tablas de enrutamiento:

1. Click en el botón de **Table Commands [Comandos de tabla].** El cuadro de diálogo de **Insert New Routing Table [Insertar nueva tabla de enrutamiento]** aparece.

2. Escriba el nombre dentro del cuadro **Routing Table [Tabla de enrutamiento]**, y luego haga click en **Submit [Enviar]**. El nombre de la tabla se almacena en la lista desplegable para usos futuros.

4.1.2 Eliminar una Tabla de Enrutamiento Existente

Para eliminar una tabla de enrutamiento existente:

1. Seleccione el nombre de la tabla de enrutamiento de la lista desplegable.

2. Click en el botón del **Table Commands [Comandos de tabla]**.

Precaución: El usuario tiene que ser cuidadoso de no eliminar la tabla de enrutamiento principal ya que esta acción puede causar problemas de conectividad.

4.1.3 Agregando Rutas Estáticas

Para agregar una ruta estática:

1. Seleccione la pestaña **Routes [Rutas]**
2. Click en el botón de **Entries Commands [Entrada de comandos]**. El cuadro de diálogo de **Insert New Route [Insertar nueva ruta]** aparece.
3.

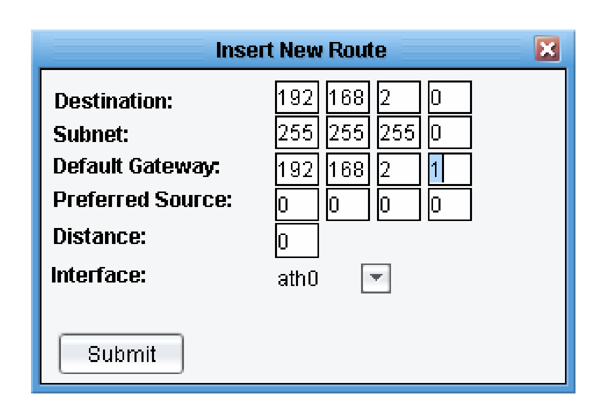


Figura 31. Insertar una nueva ruta

4. En el cuadro **Destination [Destino],** escriba la dirección de red de destino o la dirección de host de destino.
5. En el cuadro **Subnet [Sub red]**, escriba la máscara para la red de destino (255.255.255.255 para un host y 0.0.0.0 para una ruta de defecto)
6. En el cuadro **Default Gateway [Puerta de enlace predeterminada]**, escriba la dirección de la puerta de enlace predeterminada (si es necesario)
7. En el cuadro **Preferred Source [Origen preferido]**, escriba la dirección de de origen preferida que se va a comunicar con la red de destino.
8. En el cuadro **Distance [Distance]**, escriba la distancia o métrica a la red de destino (generalmente el número de saltos a la red de destino)
9. En la lista desplegable **Interface [Interfaz]**, seleccione la interfaz por el cual los paquetes van a ser enviados.
10. Para aceptar sus configuraciones, click en el botón **Submit [Enviar]** de la ventana **Insert New Route [Insertar nueva ruta]**, luego click en el botón **Submit [Submit]** del panel **IP Configuration [Configuración IP]** para completar el proceso.

4.1.4 Eliminando una ruta estática

Para eliminar una ruta estática especifica, seleccione la tabla de enrutamiento y luego haga click en el botón de Entries Commands [Entrada de comandos].

4.1.5 Modificando una ruta estática

Para modificar una ruta estática específica, seleccione la tabla de enrutamiento y luego haga click en el botón de Entries Commands [Entrada de comandos].

4.1.6 Reposicionamiento de rutas estáticas

Para modificar la prioridad de una ruta estática específica, seleccione la ruta de la tabla de enrutamiento y luego haga click en los botones para cambiar la prioridad de la ruta.

5. Wireless

NETKROM NMS le permite configurar varios parámetros inalámbricos para los nodos incluyendo lo siguiente:

- **Distancia del enlace**
- **Potencia de transmisión**
- **Modos de operación**
- **Configuraciones de la radio**
- **Parámetros de seguridad**
- **Configuraciones de acuerdo al país**
- **Operación de sondeo**

Para configurar los parámetros inalámbricos, seleccione la pestaña **Wireless** [Inalámbrico], ubicado debajo de las pestañas **Advanced Configuration of Node [Configuración avanzada del nodo], Configuration [Configuración]**. En la pestaña **Wireless [Inalámbrico]** usted puede seleccionar las sub pestañas **OpMode [Modo de operación], Radio [Radio], Security [Seguridad]** u **Outdoor [Exterior]**.

Mire la página 32 para ver un diagrama de las pestañas y sub pestañas de Advanced Configuration [Configuración Avanzada]

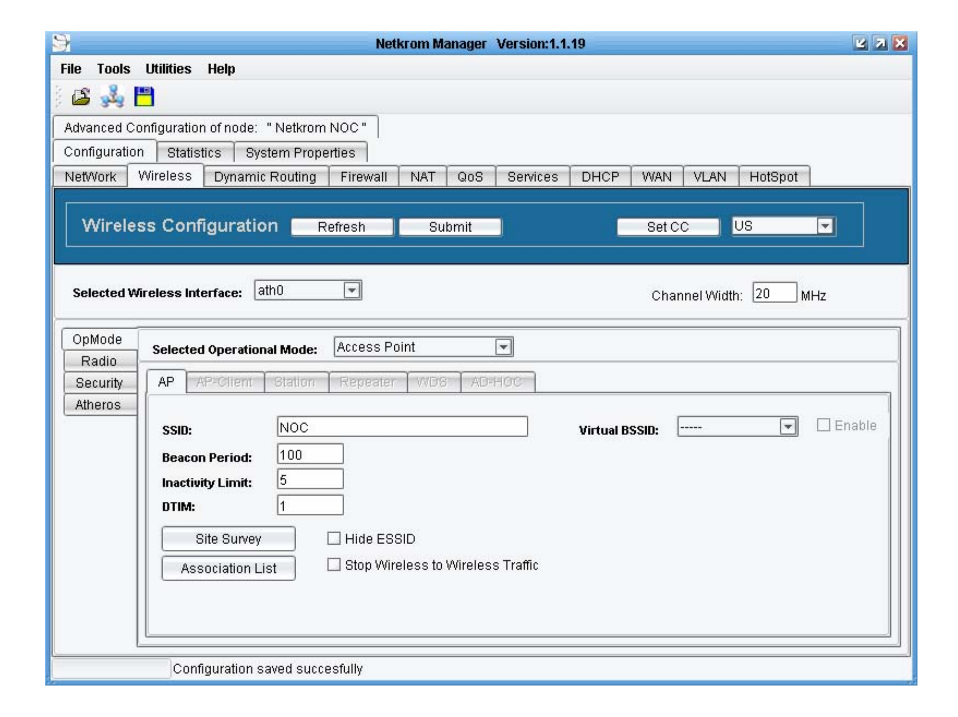


Figura 33. Panel de Wireless [Inalámbrico]

Tres botones y 2 listas desplegables están ubicadas en la parte superior de la pestaña **Wireless [Inalámbrico]:**

- **Refresh [Actualizar]** – Click en este botón para actualizar la información del nodo.
- **Submit [Enviar]** – Click en este botón para enviar y cargar la configuración al nodo.
- **Set CC [Seleccionar país] –** Click en este botón para habilitar la selección del país donde el equipo va a ser instalado.
- **CC List [Lista de países]** – Seleccione el país de la lista desplegable. Esta opción habilita algunas opciones y deshabilita otras de acuerdo a las regulaciones de cada país.
- **Selected Wireless Interface list [Lista de interfaces inalámbricas seleccionadas]** – seleccione la interfaz inalámbrica que va a ser configurada. Si hay varias interfaces inalámbricas disponibles, Esta lista desplegable muestra a todas ellas. Si la interfaz seleccionada no está active, un mensaje rojo de alerta se muestra al costado de la interfaz.

5.1 Modos de Operación

Los nodos de NETKROM tiene la habilidad de operar en los siguientes modos:

- **Punto de acceso o Access Point**
- **WDS** (Wireless Distribution System)
- **Repetidor**
- **Cliente AP**
- **Estación**

Site Survey [Sondeo]

El botón **Site Survey [Sondeo]** en todas las pestañas **OpMode [Modos de operación]**. El botón **Site Survey [Sondeo]** escanea todas las frecuencias disponibles y asociadas con los protocolos IEEE 802.11a, b y g. Cuando el escaneo se complete, el cuadro de diálogo de **Site Survey [Sondeo]** aparece, indicando cualquier fuente de interferencia creado por otros access points cercanos.

Para más información de Site Survey [Sondeo], vea la sección 5.1.6.

5.1.1 Modo operacional seleccionado

La lista desplegable **Selected Operational Mode [Modo operacional seleccionado]** muestra todos los modos que los nodos Netkrom pueden soportar. Seleccionar un modo de operación de la lista desplegable hace que la pestaña **OpMode** correspondiente esté disponible.

5.1.2 Configurar como Access Point

Para configurar el nodo como access point (AP), seleccione **Access Point [Punto de acceso]** en la lista desplegable **Selected Operation Mode [Modo de operación seleccionado]**. La pestaña **AP** se vuelve disponible. Varios parámetros deben ser configurados como se muestra en la siguiente figura:

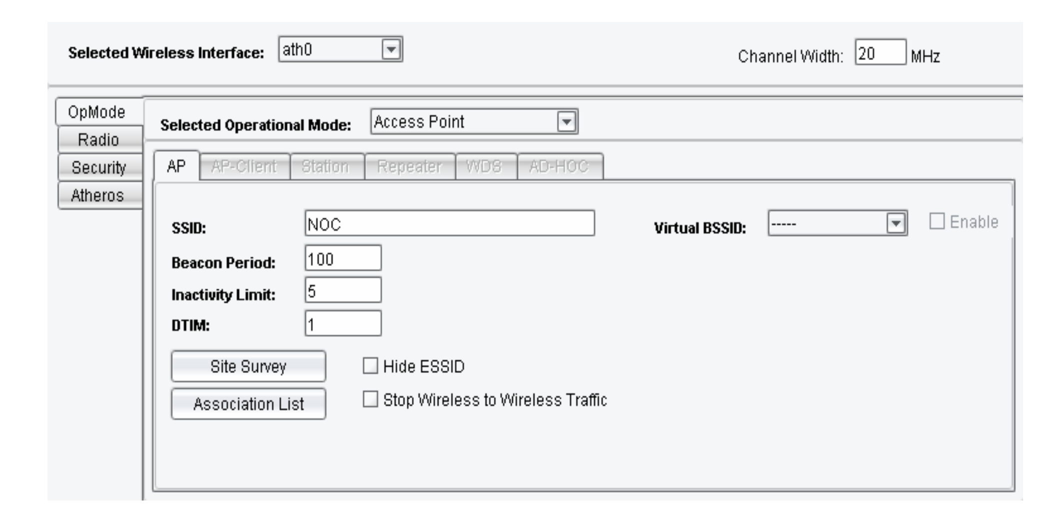


Figura 34. Modos de operación inalámbricos

SSID (Service Set Identifier)

Este campo contiene el nombre de la red inalámbrica que va a ser publicado por el access point. Escriba el nombre dentro del cuadro **SSID**.

Inactivity Limit [Límite de inactividad]

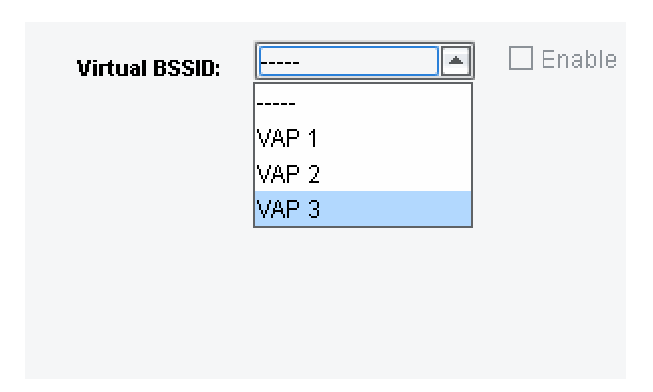
Si la conexión entre una estación asociada con el access point se pierde por un tiempo mayor al límite de inactividad, el access point envía una trama de des asociación a la estación para informarle que ha sido desasociado debido a su tiempo de inactividad. Para configurar el **Inactivity Limit [Límite de inactividad]**, escriba el valor en minutos del tiempo en el cuadro correspondiente.

Periodo de Broadcast del SSID

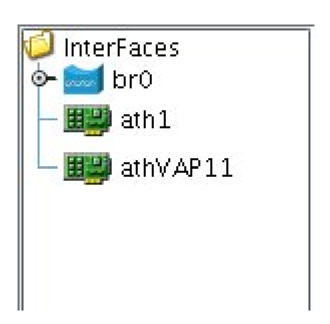
Este campo representa el intervalo de tiempo deseado entre dos broadcast del SSID. Para configurar este parámetro llene el cuadro **Beacon Period [Periodo de Broadcast del SSID]**, con el tiempo en segundos deseado. (Por defecto: 100)

Virtual BSSID [BSSID Virtual]

Usted puede crear SSID virtuales desde una interfaz física. Primer usted tiene que configurar la interfaz física (periodo de broadcast del SSID, límite de inactividad, etc.). Estos parámetros van a ser los mismos en el VAP.



Para crear un VAP haga click en la barra desplegable **Virtual BSSID [BSSID Virtual]**, elija VAP 1 y haga click en **Enable [Habilitar]** para habilitarlo. Después de hacer click en **submit [Enviar]** se creará una interfaz virtual.



Lista de Asociación

Para accede a la lista de información de todos los nodos asociados con el AP, click en el botón **Association List [Lista de asociación]**. Un cuadro de diálogo aparece.

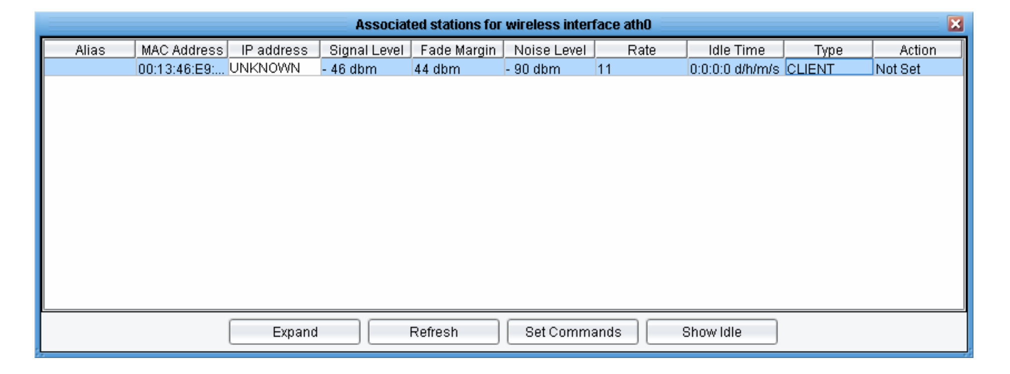


Figura 35. Lista de asociación

En la ventana se muestra la siguiente información de cada nodo asociado:

Alias [Alias]

Es un nombre especial que usted puede crear para identificar a un cliente en el AP.

MAC Address [Dirección MAC]

Muestra la dirección MAC de los nodos asociados.

IP Address [Dirección IP]

Muestra la dirección IP del nodo asociado al AP.

Signal Level [Nivel de señal]

Muestra el nivel de señal de los nodos asociados.

Fade Margin [Margen de desvanecimiento]

Muestra la diferencia entre el nivel de señal y el nivel de ruido.

Noise Level [Nivel de ruido]

Muestra el nivel de ruido de acuerdo al nodo correspondiente.

Rate [Velocidad]

Muestra la velocidad que el AP usa para intercambiar datos con cada nodo cliente.

Idle Time [Tiempo de inactividad]

Muestra el tiempo que ha pasado desde que el nodo cliente fue desasociado.

Type [Tipo]

Muestra el tipo de nodo. Puede mostrar cualquiera de los siguientes valores:

- Adapter (Modo estación)
- AP_Client (Modo cliente AP)
- WDS_Type
- Client (cliente)

Action [Acción]

- Este campo es una lista desplegable que le permite llevar a cabo varios tipos de acciones diferentes, por ejemplo usted puede:

- Seleccionar **Set Alias [Configurar Alias]** para configurar un alias a un nodo específico.

- Seleccionar **Remove [Eliminar]** para eliminar un nodo inactive de la lista.

- Seleccionar **Disassociate [Desasociar]** para desasociar un cliente que está asociado con el AP.

- Seleccionar **Permanent Disassociation [Desasociación permanente]** para desasociar un cliente que está asociado al AP y simultáneamente agregar su MAC a la lista de control de acceso y denegarle el acceso.

Stealth Mode [Modo Sigiloso]

Cuando está habilitado, el AP no transmite broadcast del SSID y oculta su SSID lo cual lo hace invisible. Ningún otro nodo puede descubrirlo a menos que el nodo tenga la configuración del AP. In Además, un protocolo de sondeo es implementado, el cual es compatible con enlaces entre APs y clientes Netkrom. Cuando se usa este protocolo, los clientes Netkrom son capaces de detectar los APs en modo sigiloso.

Para implementar esta característica, seleccione la casilla **Stealth Mode [Modo Sigiloso]**.

Hide Essid

Esconder el ESSID del AP previene que usuarios exteriores se unan a la red ya que ellos no pueden detector el nombre de la red inalámbrica. Para que el AP para de publicar su SSID, seleccione la casilla **Hide ESSID [Ocultar ESSID]**.

Parar el tráfico de Wireless a Wireless

Para el tráfico entre dos estaciones inalámbricas que están asociadas con un AP, seleccione la casilla **Stop Wireless to Wireless Traffic [Parar el tráfico de wireless a wireless**.

5.1.3 Configurando el Modo WDS

Un nodo Netkrom puede operar como un access point WDS. Esto le da la oportunidad de configurar una red inalámbrica de sistema distribuido mediante la configuración de un número de nodos NETKROM WDS. Todas las características y configuraciones descritas en la sección del access point son soportadas en el modo WDS. Además el modo WDS cuenta con una os los nodos WDS incluidos en la red.

Para configurar un nodo con el modo WDS, seleccione **WDS** de la lista desplegable **Selected Operation Mode [Modo de operación seleccionado]**. La pestaña **WDS** se vuelve disponible. Los campos **SSID [Nombre de la red inalámbrica], Inactivity Limit [Límite de inactividad], Beacon Period [Periodo de broadcast del SSID], Site Survey [Sondeo], Stealth Mode [Modo Sigiloso], Hide ESSID [Ocultar ESSID] y Stop Wireless to Wireless Traffic [Parar tráfico wireless a wireless]** se configuran de la misma manera que el modo access point. La pestaña WDS también cuenta con el botón **Association List [Lista de Asociación]** y una lista de **Registered WDS Nodes [Nodos WDS Registrados].**

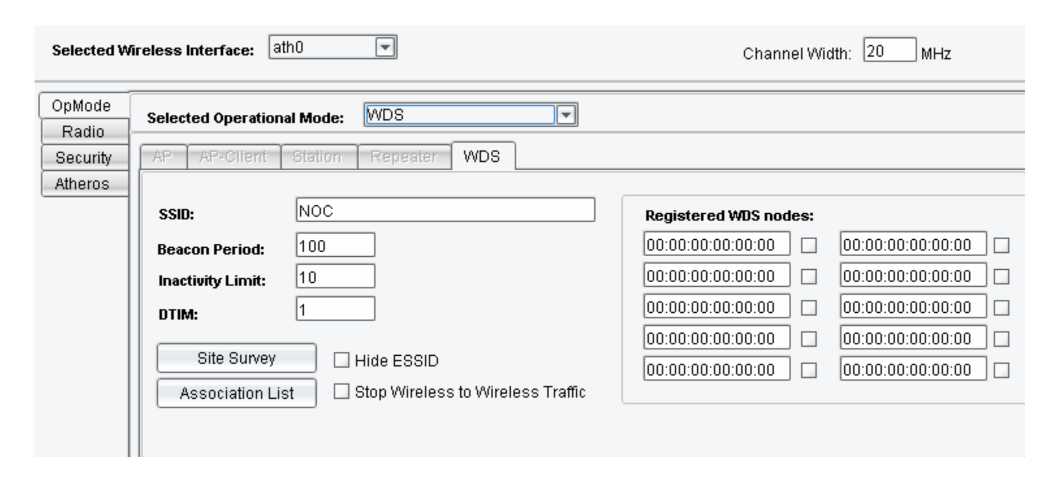


Figura 36. Modo WDS

En la lista de **Registered WDS nodes [Nodos WDS Registrados],** escriba la dirección MAC de los nodos que van a ser configurados. Seleccione la casilla junto a la dirección MAC para habilitar el nodo dentro de la red WDS. (Esta característica puede ser útil cuando los nodos WDS cambian de comportamiento. Usted puede mantener las direcciones Mac de los nodos en la lista y habilitarlos o deshabilitarlos cuando sea necesario.

5.1.4 Configurar el Modo Repetidor

El modo repetidor es un modo avanzado de Netkrom. Cuando un nodo NETKROM está configurado como un repetidor, este opera como un cliente. Se asocia con un AP y adopta sus parámetros. Después de la asociación se complete, NETKROM repite el BSS creando una extensión del BSS. Los repetidores implementan una combinación de ambos el modo cliente y el modo access point y cuenta con el modo sigiloso y control de tráfico inalámbrico.

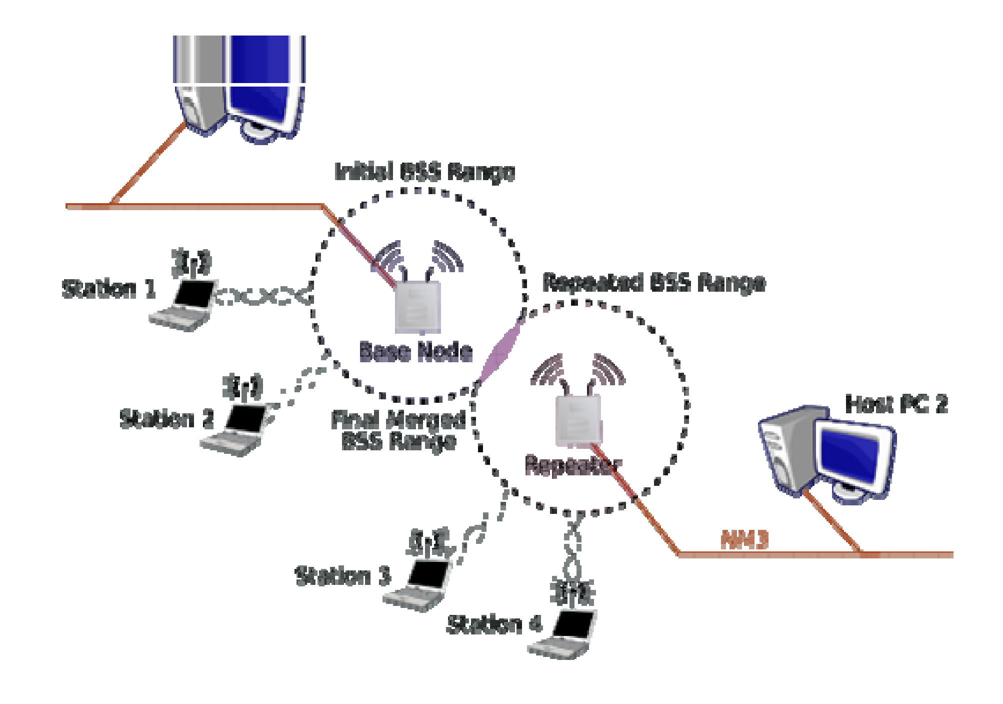


Figura 37. Modo Repetidor

Como se ilustra en el diagrama de arriba, un repetidor Netkrom está asociado con un nodo base. Después de ser asociado, el repetidor NETKROM expande el BSS de nodo base. Como resultado el rango inicial BSS se expande gracias al repetidor.

Preferred SSID/Preferred BSSID [SSID Preferida/BSSID Preferida]

Para configurar un nodo Netkrom como repetidor, escriba el nombre de **Preferred SSID [SSID Preferida]** o la dirección MAC **Preferred BSSID [BSSID Preferida]** dentro de los campos mencionados. Click en **Submit [Enviar]** y espere que el repetidor se asocie con el nodo base especificado. Ahora el repetidor está listo para aceptar asociaciones con estaciones inalámbricas.

Link Quality [Calidad de Enlace] y Signal Level [Nivel de Señal]

Los campos **Link Quality [Calidad del Enlace] y Signal Level [Nivel de Señal]** muestran información de la asociación establecida. En el caso del primer campo muestra la calidad del enlace mientras que el segundo el nivel de la señal captada por el repetidor.

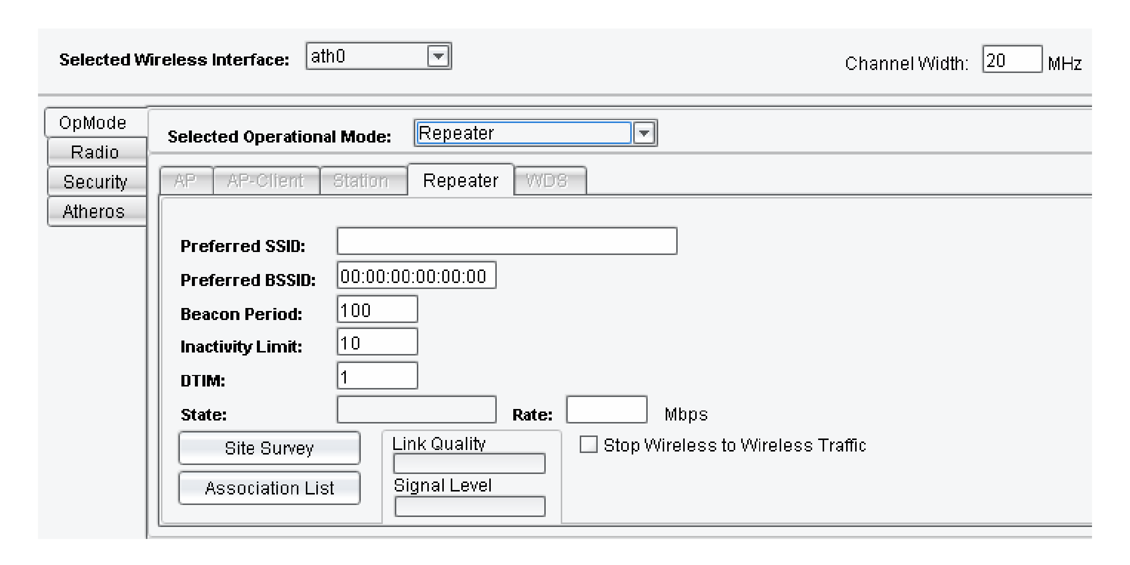


Figura 38.Configuración del Modo Repetidor

5.1.5 Configurar el Modo Cliente AP y Estación

Los modos **AP Client [Cliente AP]** y **Station [Estación]** son similares. Ambos modos configuran el nodo como cliente. La diferencia principal es que el modo **AP Client [Cliente AP]** soporta 4 direcciones de tráfico. El modo **Station [Estación]** tiene un proxy-ARP que soporta solo 3 direcciones de tráfico. Seleccione el modo de acuerdo a su necesidad.

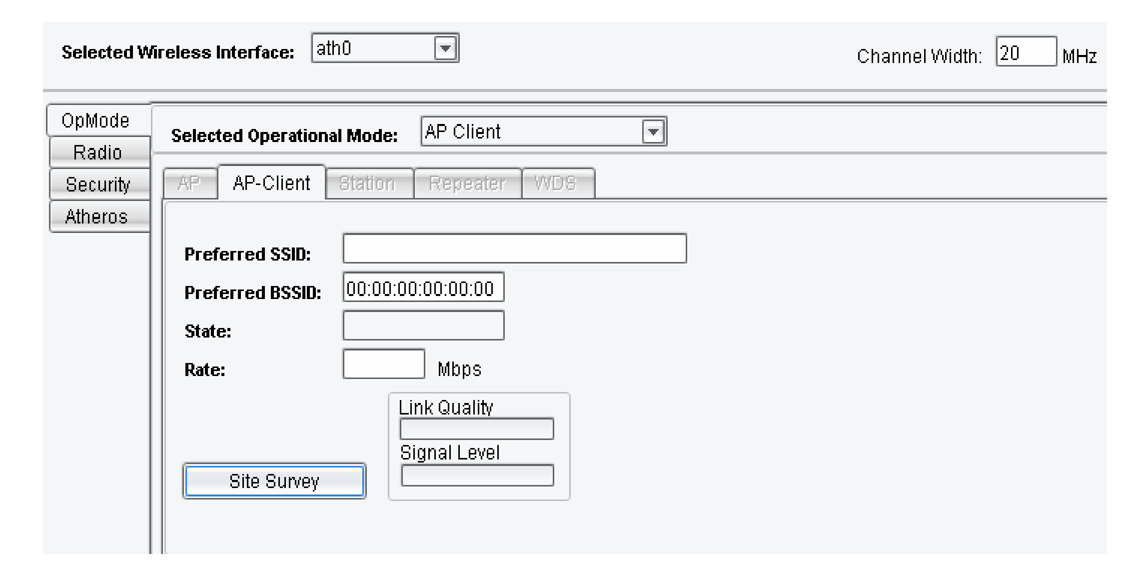


Figura 39. Configuración del Modo Cliente AP

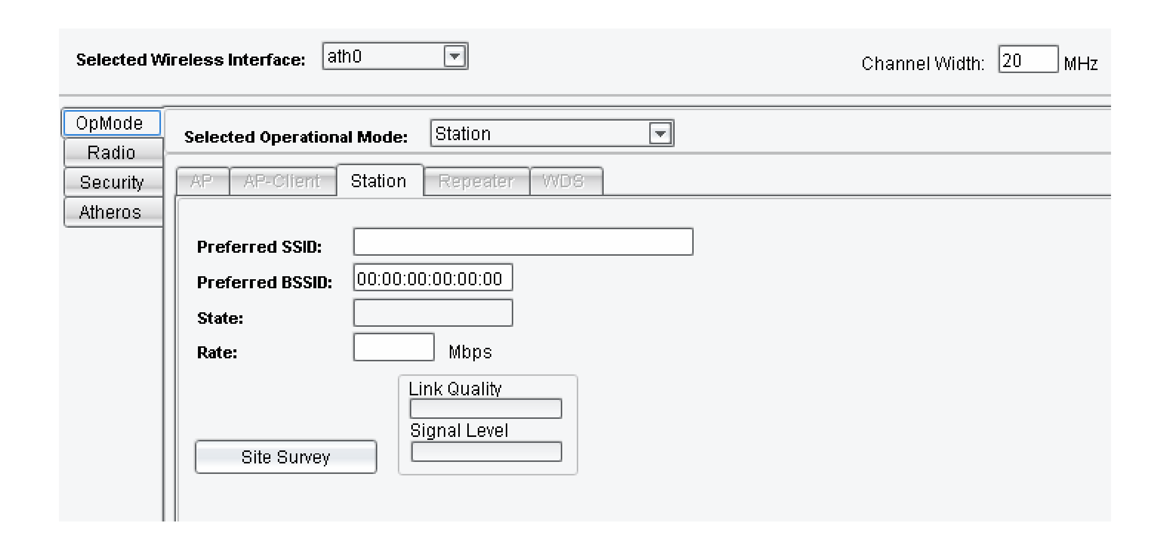


Figura 40. Configuración del Modo Estación

Preferred SSID [SSID Preferida]

Este campo contiene el nombre del ESSID publicado por el nodo AP. Escriba el nombre del SSID del AP al cual se unirá.

Preferred BSSID [BSSID Preferida]

Este campo contiene el BSSID del nodo AP. Escriba la dirección MAC del AP al cual se unirá.

Link Quality [Calidad de Enlace] y Signal Level [Nivel de Señal]

Los campos **Link Quality [Calidad del Enlace] y Signal Level [Nivel de Señal]** muestran información de la asociación establecida. En el caso del primer campo muestra la calidad del enlace mientras que el segundo el nivel de la señal captada por el repetidor.

5.1.6 Usando la Operación Site Survey [Sondeo]

El botón **Site Survey [Sondeo]** está disponible en todos los modos AP, AP Client [Cliente AP], Repeater [Repetidor] y Station [Estación], el Site Survey [Sondeo] escaneará todos los canales para encontrar redes inalámbricas disponibles al cual unirse. Cuando un nodo está en modo access point o WDS, el Site Survey [Sondeo] puede ser usado para escanear canales usados e interferencia de otros access points.

Después de hacer click en el botón Site Survey [Sondeo], un cuadro de diálogo aparece mostrando todas la redes escaneadas disponibles.

Después de que el escaneo se complete y el cuadro de diálogo se llena, la barra de estado en la parte inferior del of NETKROM NMS muestra el mensaje **Site survey list retrieved successfully [Sondeo exitoso]**.

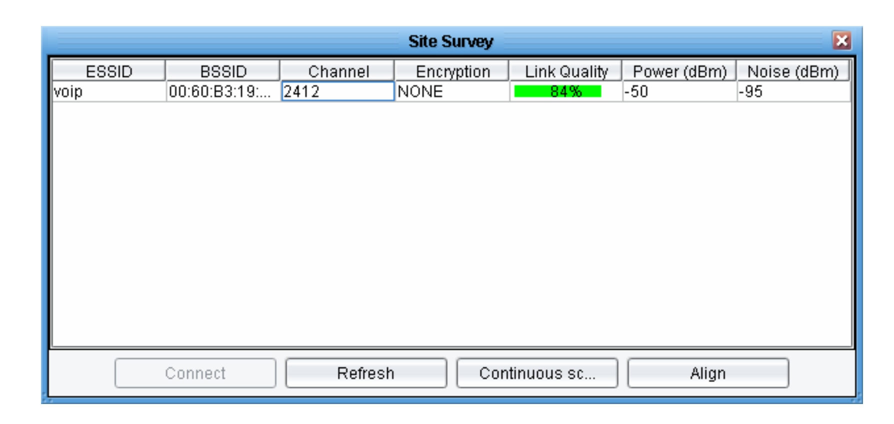


Figura 41. Operación de Sondeo

En la parte inferior del cuadro de Site Survey [Sondeo] aparecen los siguientes botones:

Connect [Conectar]:

Seleccione un nodo y haga click en este botón para unirse al nodo seleccionado.

Refresh [Actualizar]

Click en este botón para volver a escanear los nodos disponibles.

Continuous Scan [Escaneo Continuo]

Click en este botón para habilitar un escaneo continuo. El escaneo se lleva a cabo hasta presionar por segunda vez este botón.

Align [Alineación]

Esta opción le permite lograr la máxima alineación para su enlace. Después de hacer click en este botón aparece un cuadro de diálogo. Este cuadro de diálogo muestra los campos **BSSID**, **SSID**, **Channel Number [Número de Canal]**, **Link Quality [Calidad del Enlace]** y **Signal Level [Nivel de Señal]**. Usando esta ventana usted puede monitorear el nivel de la intensidad de la señal. Después de lograr la máxima alineación entre sus equipos, haga click en **Quit [Salir]** para abandonar la ventana de alineación.

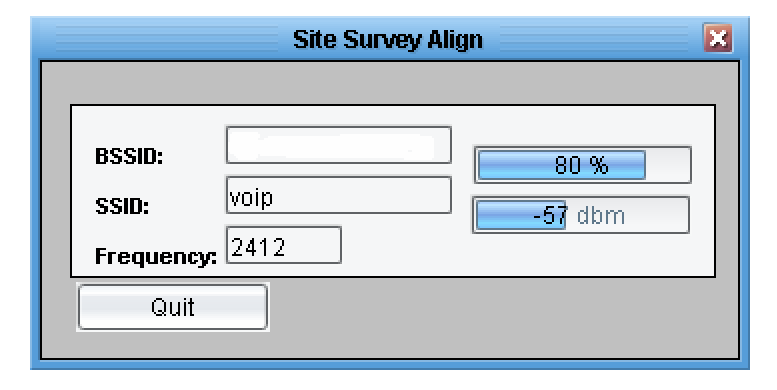


Figura 42. Ventana de Alineación

5.2 Configurando los Parámetros de la Radio

Para configurar los parámetros de la radio de la interfaz inalámbrica seleccionada, seleccione la pestaña **Radio** del panel **Wireless [Inalámbrico]**. Usted puede configurar:

- Seleccionar el protocolo (IEEE 802.11a, b y g)
- Seleccionar el número de canal o frecuencia
- Seleccionar la velocidad de transmisión
- Habilitar la suplantación de identidad
- configurar la dirección MAC
- Habilitar la diversidad
- Seleccionar el conector de la antena

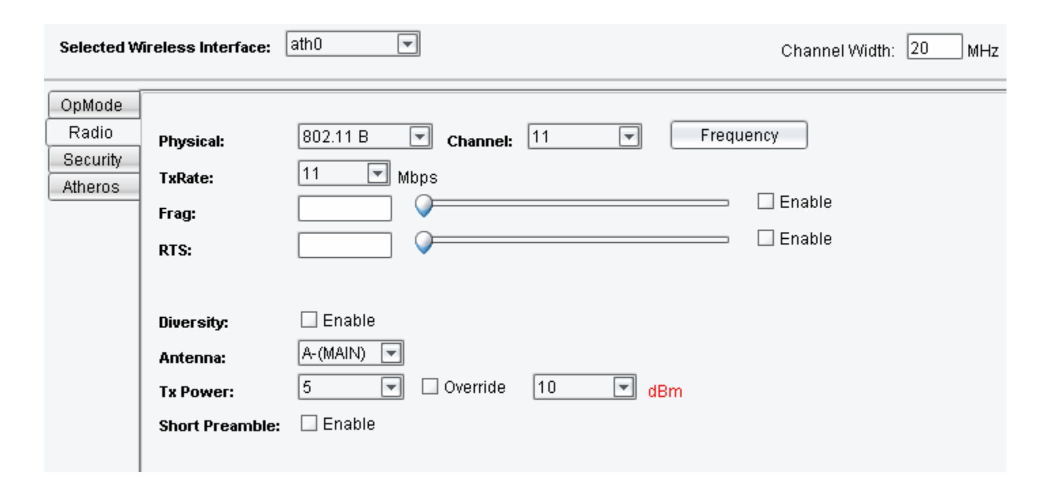


Figura 43. Configuración de los Parámetros de la Radio

5.2.1 Seleccionado el Protocolo WiFi

La lista desplegable **Physical [Físico]** contiene una lista de todos los protocolos disponibles para su MBROMB. Si su hardware soporta los protocolos IEEE 802.11 a, b y g, la lista desplegable contendrá las opciones **AUTO, 802.11A, 802.11B, 802.11B-G, Turbo A y Turbo G.**

5.2.2 Configurar los Canales y Frecuencias

La lista desplegable **Channel [Canal]** muestra el canal de radio seleccionado. Para convertir el canal en frecuencia click en el botón **Frequency [Frecuencia]**.

5.2.3 Configurar la Velocidad de Transmisión

La lista desplegable **TxRate [Velocidad de Transmisión]** le permite seleccionar la velocidad de transmisión basados de acuerdo al protocolo wifi seleccionado. Usted también puede seleccionar la opción **Auto**. En el modo Auto NETKROM se auto configurará para soportar la velocidad de transmisión óptima para cada nodo. Esta opción es muy útil en ambientes sensibles. En el modo Auto se usa un algoritmo avanzado el cual determina la velocidad de transmisión.

Nota: *Las tramas de control y administración siempre son transmitidas a la velocidad más baja disponible de acuerdo al protocolo wifi seleccionado.*

5.2.4 Configurando la Dirección MAC

El campo **MAC Address [Dirección MAC]** contiene la dirección MAC del radio seleccionado. Sin embargo, usted puede habilitar el Spoofing [Suplantación de Identidad] para configurar una nueva dirección MAC.

5.2.5 Configurando la Fragmentación

El campo **Frag** le permite implementar la fragmentación de paquetes, una técnica que mejora el rendimiento de la red en presencia de interferencia. Usted puede configurar el tamaño de la fragmentación escribiendo el valor en bytes en el campo **Frag**. Si una trama excede este valor entonces será fragmentada. El rango de fragmentación es entre 256 a 2048 bytes. Configurar la fragmentación a 2048 deshabilitará la fragmentación.

Para habilitar la fragmentación habilite la casilla **Frag** y luego escriba el valor de la fragmentación en bytes.

5.2.6 Configurando el RTS

El campo **RTS** le permite implementar el RTS/CTS entre un nodo Netkrom y otra estación inalámbrica. RTS/CTS ayuda a minimizar las colisiones entre estaciones ocultas en una red inalámbrica. El RTS/CTS hace que el nodo envíe una trama Ready To Send al destino, luego espera que el destino responda con una trama Clear To Send. Luego el nodo de origen enviará sus datos que tiene que enviar. El RTS/CTS puede ayudar a evitar las colisiones. Cuando implementa el RTS en un access point NETKROM, la operación de RTS la operación se inicia cuando un paquete excede el valor configurado en el campo **RTS**. El rango válido es desde 0 a 2347 bytes. (Si RTS está habilitado se recomienda un valor inicial de 500.)

Para habilitar el **RTS**, habilite la casilla **RTS** y luego escriba el valor en bytes dentro del campo.

5.2.7 Seleccionando la Opción de Diversidad

El campo **Diversity [Diversidad]** le permite habilitar el uso de dos antenas para la operación de diversidad si las dos antenas se usan para la misma radio.

5.2.8 Seleccionando la Antena

La lista desplegable **Antenna [Antena]** le permite seleccionar la antena a ser usada **Right [Derecha] o Left [Izquierda].**

.

5.2.9 Configurando la Potencia de Transmisión

La potencia de transmisión puede ser configurada desde 5 hasta 30. Para configurar la potencia de transmisión, seleccione un valor de la lista desplegable **Tx Power [Potencia de Transmisión]**.

5.3 Configurando los Parámetros de Seguridad

Desde la pestaña **Security [Seguridad]** usted puede configurar los parámetros de seguridad de la interfaz inalámbrica seleccionada. Desde esta pestaña usted puede configurar lo siguiente:

- **WEP** (Wired Equivalent Privacy)
- **WPA** (Wi-Fi Protected Access)
- **ACL** (Access Control List)

5.3.1 WEP

En la pestaña **WEP** usted puede configurar el protocolo WEP. Para implementar el protocolo WEP, seleccione **WEP** de la lista desplegable **Selected Encryption Mode [Modo de Encriptación seleccionado]**

Para implementar la encriptación 64 bits, seleccione **WEP-64** en la lista desplegable **WEP Type [Tipo WEP]**.

Para implementar la encriptación 128 bits, seleccione **WEP-128** en la lista desplegable **WEP Type [Tipo WEP]**.

Cuatro cuadros de texto (**WEP Key #1, #2, #3** and **#4)** con botones adyacentes le permite mantener cuatro contraseñas de encriptación diferentes, mientras se usa uno de ellos. Escriba uno o más contraseñas dentro de los cuadros de texto, y luego seleccione la que va a ser usada haciendo click el botón circular adyacente.

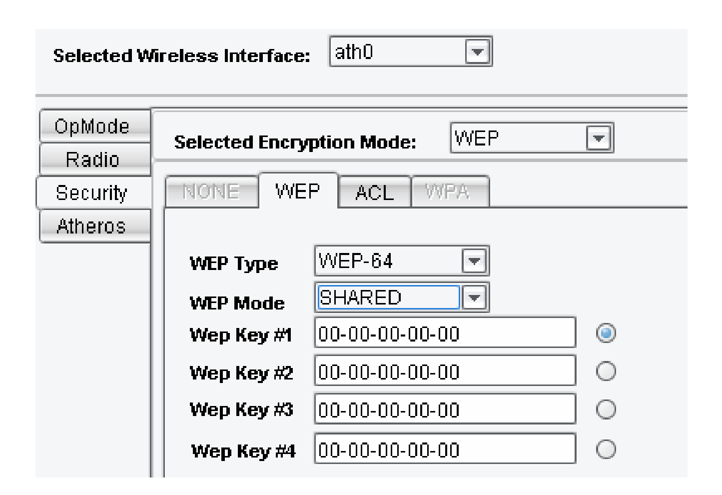


Figura 44. Configuración de WEP

5.3.2 Configurando WPA

En la pestaña **WPA** usted puede configurar un nodo con el protocolo WPA. Para implementar WPA, seleccione **WPA** en la lista desplegable **Selected Encryption Mode [Modo de Encriptación Seleccionado]**.

Puede seleccionar entre el protocolo WPA y WPA2 en **WPA Mode [Modo WPA]**.

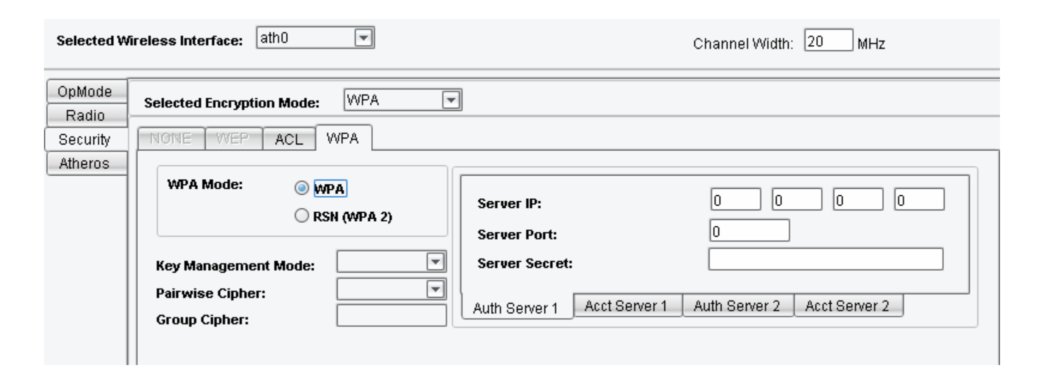


Figura 45. Configuración de WPA

Configurando el Key Management Mode [Modo de Administración de Contraseña]

En esta lista desplegable puede seleccionar entre **PSK** (Pre-Shared Key) o **EAP** (Extensible Authentication Protocol). Esta selección determina los campos que aparecerán en el lado derecho del panel.

EAP

Cuando se selecciona EAP, varios cuadros de texto aparecen en el lado derecho del panel. Estos campos se requieren para forzar al access point NETKROM a autenticar a los clientes en un servidor de autenticación. Los cuadros de textos incluyen:

- **Server IP [IP del Servidor]:** es la dirección IP del servidor de autenticación.
- El **Server Port [Puerto del Servidor]** es el número de Puerto usado para las transacciones de paquetes EAP-TLS (usualmente 1812)
- Un **Server Secret [Secreto del Servidor]** el cual es una frase que es usada por el nodo NETKROM para ser aceptado por el servidor de autenticación.

*EAP-TLS es por defecto el protocolo compatible con EAP. Los nodos NETKROM usan 802-1X para autenticar a sus clientes. Si el nodo NETKROM está configurado como un cliente, en el caso de uso de EAP-TLS, usted debe cargar los certificados apropiados en la estación NETKROM. Esto se puede hacer haciendo click en **Upload Server [Servidor de Subida]** y **Client Certificate [Certificado de Cliente]** en el panel derecho.*

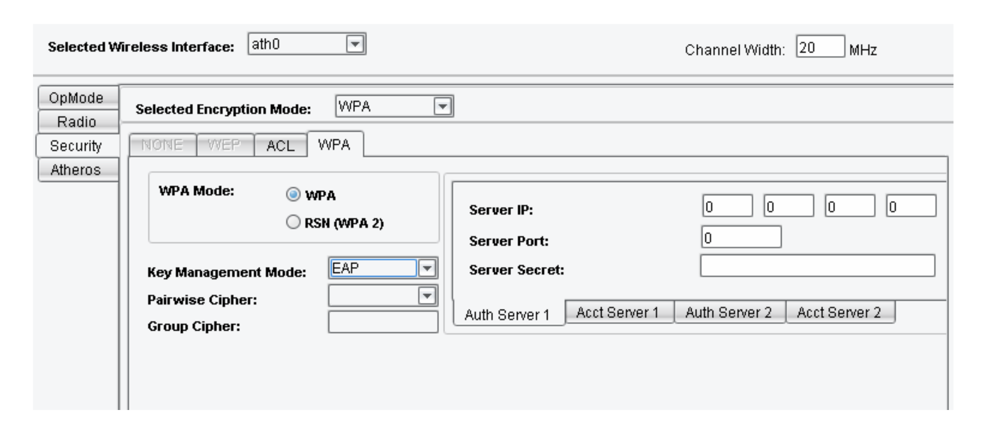


Figura 46. Configuración de EAP

PSK

Cuando **PSK** es seleccionado de la lista desplegable **Key Management Mode [Modo de administración de contraseñas]**, el cuadro **Pass Phrase [Frase de Paso]** aparece en el lado derecho del panel. Este es el valor inicial en las cuales las contraseñas WPA negociadas son creadas.

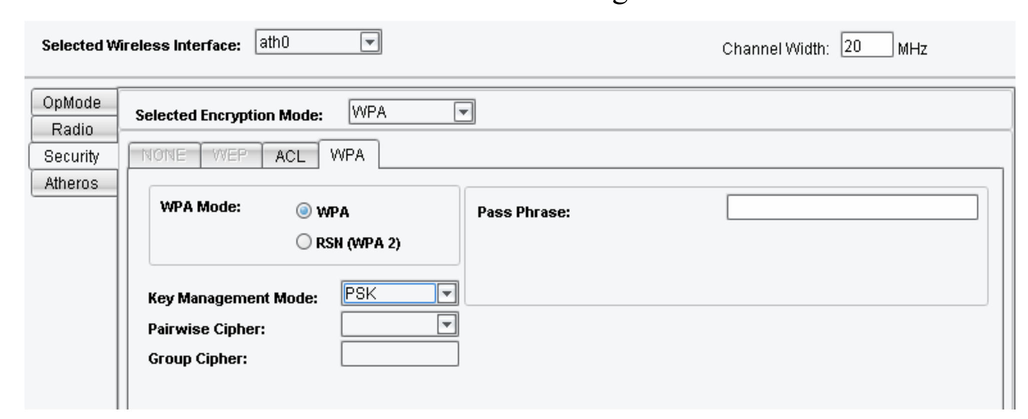


Figura 47. Configuración de PSK

Pairwise Cipher

Proporciona tres tipos de encriptación:.

- **TKIP** (Temporal Key Integrity Protocol)
- **AES (CCMP)** (Advanced Encryption Standard-Counter Mode CBC-MAC Protocol)
- **BOTH** (seleccionado si el nodo NETKROM está configurado como access point)

Group Cipher

(Group Cipher no está habilitado en el NETKROM NMS versión 1.1.3)

5.3.3 Configurando Listas de Control de Acceso (ACL)

Cuando el modo de operación ha sido configurado en **Access Point** o **WDS,** la sub pestaña **ACL** en la pestaña **Security [Seguridad]** está disponible. Usted tiene la opción de configurar una lista de control de acceso para administrar a los clientes que se van a conectar o no al access point

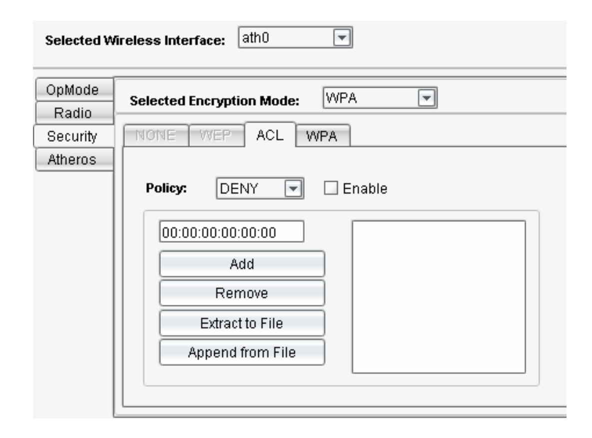


Figura 48. Configuración de una lista de control de acceso

Denegando el Acceso

Para denegar que clientes específicos accedan al nodo, seleccione **DENY [Denegar]** de la lista desplegable **Policy [Política].** Clientes con dirección MAC que concuerden con las direcciones MAC registradas en el ACL se les denegará el acceso. Todas las otras direcciones serán permitidas.

Permitiendo el Acceso

Para permitir que clientes específicos accedan al nodo, seleccione **ALLOW [Permitir]** de la lista desplegable **Policy [Política].** Clientes con dirección MAC que concuerden con las direcciones MAC registradas en el ACL se les permitirá el acceso. Todas las otras direcciones serán denegadas.

Creación de Listas de Control de Acceso

Hay dos métodos para crear una ACL.

- Escriba las direcciones MAC manualmente, use el botón **Add [Agregar]** para agregarla a la ACL, o **Remove [Eliminar]** para eliminarla de la ACL.

- Cargue un archive de texto conteniendo las direcciones MAC usando el botón **Append from File [Anexar desde Archivo]**.

Guardando Listas de Control de Acceso

Para guardar una ACL, click en **Extract to File [Extraer a Archivo]** para guardar la ACL como un archivo. Esta característica es útil si usted necesita utilizar la misma ACL en otro access point.

5.4 Configurando Las Capacidades Avanzadas de Atheros

La pestaña Atheros es útil para optimizar la operación de los nodos NETKROM de acuerdo a la distancia.

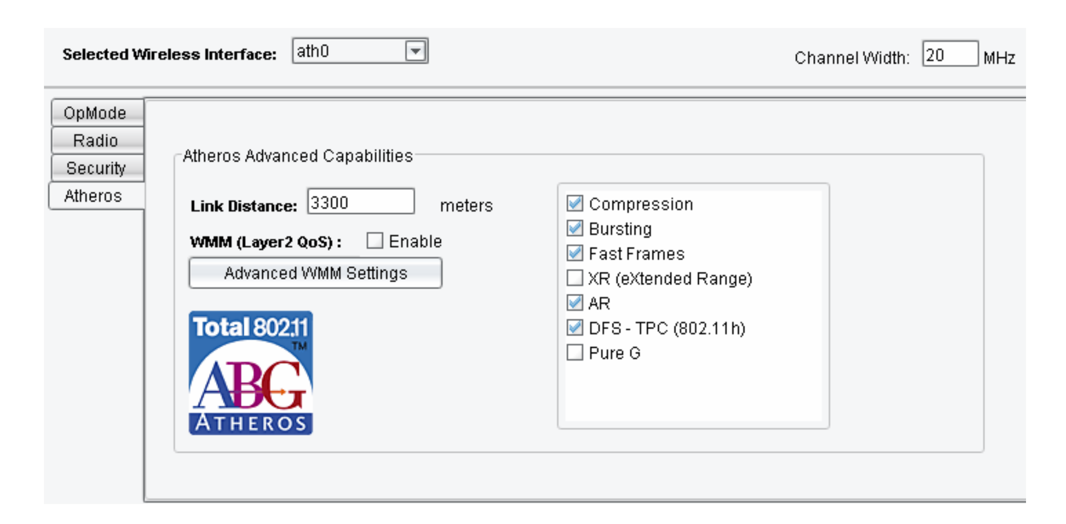


Figura 49. Configuraciones Avanzadas de Atheros

Link Distance [Distancia del Enlace]

Configurar la distancia del enlace puede ser efectivo al optimizar la operación de un nodo. Cuando la distancia del enlace se define, el ACK de espera se configure de acuerdo a la distancia. En ambientes con pérdidas donde muchos intentos ocurren, el ACK de espera debe ser configurado de acuerdo a la distancia entre los nodos. Para configurar este parámetro, escriba la distancia (en metros) dentro del cuadro de texto **Link Distance [Distancia del Enlace]**.

Fast Frames

Fast Frames es una característica avanzada de Atheros que utiliza la agregación de tramas para incrementar el throughput del sistema. Esto incrementa el throughput mediante la transmisión de más datos por trama y eliminando las pausas entre tramas. Para implementar el fast frames, seleccione la casilla **Fast Frames**.

Packet Bursting

Packet Bursting es otra técnica usada por Atheros que incrementa el throughput mediante la disminución del overhead y enviando más tramas por periodo determinado de tiempo. Para implementarlo, seleccione la casilla **Packet Bursting**.

Advanced WMM Settings [Configuraciones Avanzadas de WiFi Multimedia]

WMM (Wi-Fi Multimedia) es una técnica de calidad de servicio basado en la prioridad usado en la implementación de voz sobre WLANs. Para implementar WMM, seleccione la casilla **WMM (Layer QoS),** luego haga click en **Advanced WMM Settings** para acceder a la siguiente ventana.

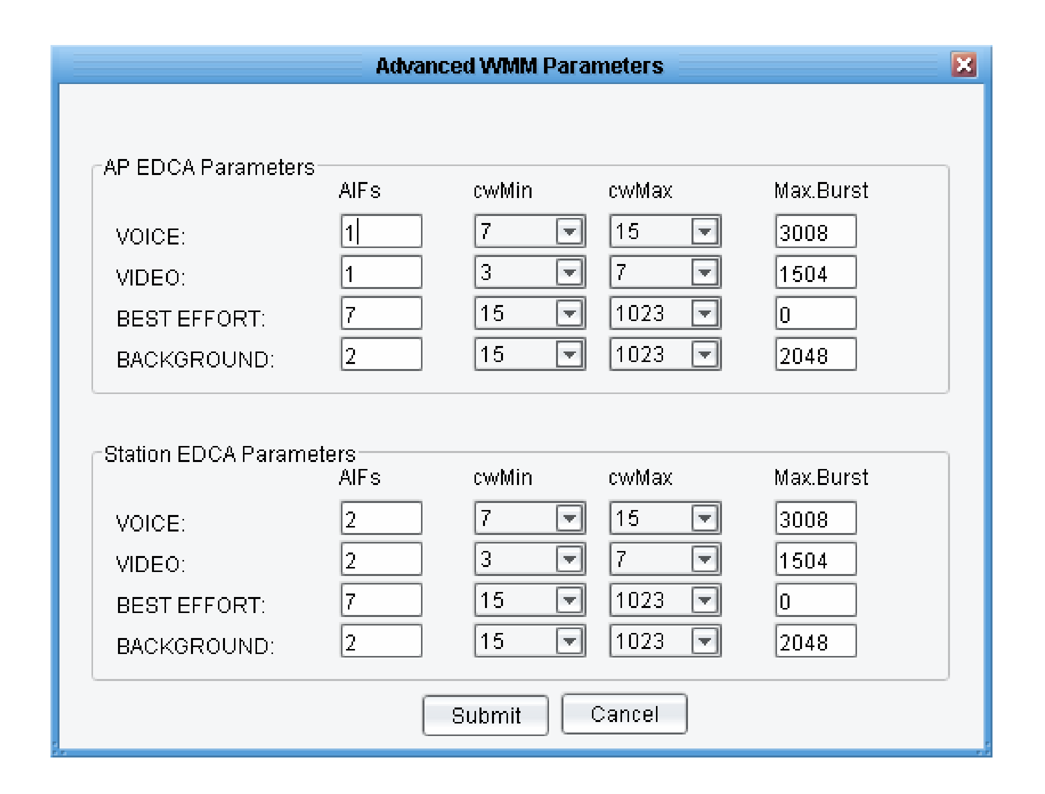


Figura 50. Parámetros Avanzados WMM

Colas WMM (Prioridades de Tráfico)

Hay cuatro colas que el hardware usa para organizar y priorizar los paquetes.

AC_BK= Background Access Category

(La más baja prioridad para los datos. No requiere sensibilidad de tiempo como por ejemplo FTP)

AC_BE= Best Effort Access Category

(Prioridad media, por ejemplo datos tradicionales IP)

AC_VI= Video Access Category

(Alta prioridad, por ejemplo Video)

AC_VO= Voice Access Category

(La más alta prioridad, Por ejemplo VOIP y streaming media)

NOTA1: A favor del access point AP estos campos son publicados en el Beacon y los clientes y estacione lado son informados con el fin de conocer las políticas del AP. Por otro lado el AP conoce las políticas de cada cliente.

NOTA2: Los parámetros AP afectan el flujo del tráfico desde el AP hacia los clientes o estaciones (por otro lado STA EDCA controla el upstream desde los clientes o estaciones hacia el AP).

Campos Configurables (Por cola)

.

a.**CWmin** = Minimum Value of Contention Window

b.**CWmax** = Maximum Value of Contention Window

b.**AIFsn** = Arbritary Interframe Space

d.**TXOP** = Length of TXOP

CWmin
Entrada al algoritmo que especifica el tiempo de espera random backoff inicial para un intento de retransmisión. Este valor es el límite inferior expresado en milisegundos.

CWmax
Este valor es el límite superior expresado en milisegundos para el valor de doubling random backoff. Este doubling continúa hasta que las tramas de datos se envíen o el Max Contention Window se alcance.

AIFs

Especifica un tiempo de espera para las tramas de datos.

TXOP
Este es el intervalo de tiempo en el cual una estación o cliente **WMM** tiene el derecho de iniciar transmisiones dentro del medio inalámbrico.

5.5 Topologías y Escenarios Inalámbricos

En esta sección se describen dos topologías y escenarios inalámbricos, basados en los modos operacionales de NETKROM. En la primera sección se describen dos maneras de configurar un enlace punto a punto. En la segunda sección se describe una topología concerniente al modo repetidor de NETKROM.

5.5.1 Enlace Punto a Punto

Hay dos escenarios de topología básicos. Usted puede crear un enlace punto a punto usando cualquiera de los escenarios.

Escenario WDS a WDS

un enlace punto a punto se puede crear con dos nodos NETKROM como access points WDS.

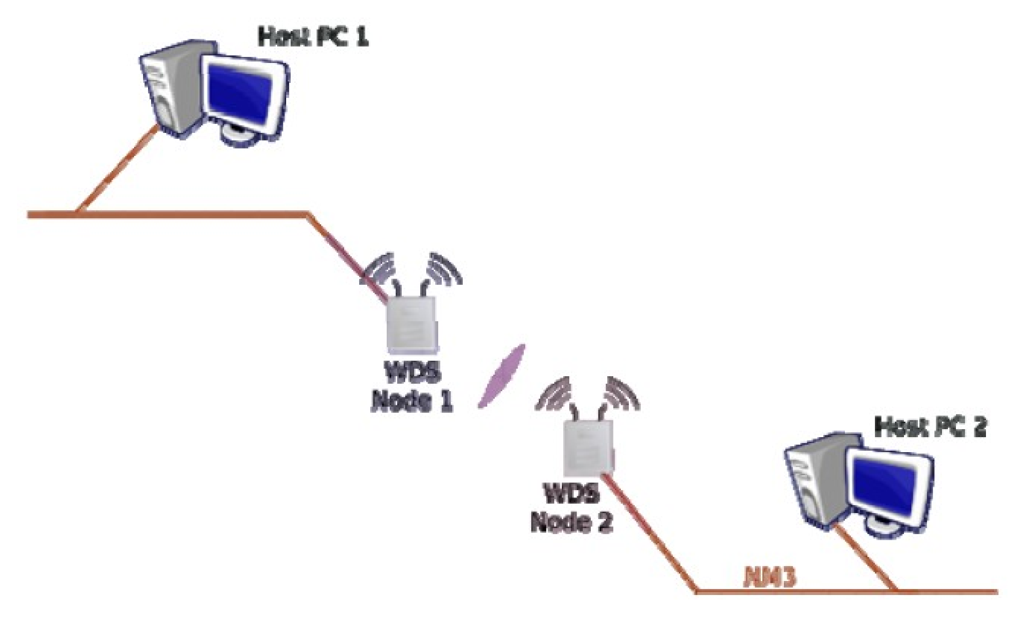


Figura 51. Enlace PTP con 2 WDS

La configuración del nodo 1 WDS debería ser como sigue:

- La dirección MAC del nodo 2 WDS debe ser configurada en la lista del nodo 1 WDS.
- Ambos nodos. Deben transmitir en la misma frecuencia.
- El modo sigiloso de NETKROM debería ser usado (si usted desea evitar la transmisión de beacoms) o ocultar el SSID.
- Adicionalmente, usted puede habilitar una ACL con políticas para denegar y permitir nodos.

La misma configuración debería ser hecha en el nodo 2 WDS, con los valores correspondientes.

Escenario AP con Cliente AP

Usted puede configurar un enlace punto a punto usando un cliente AP y un AP.

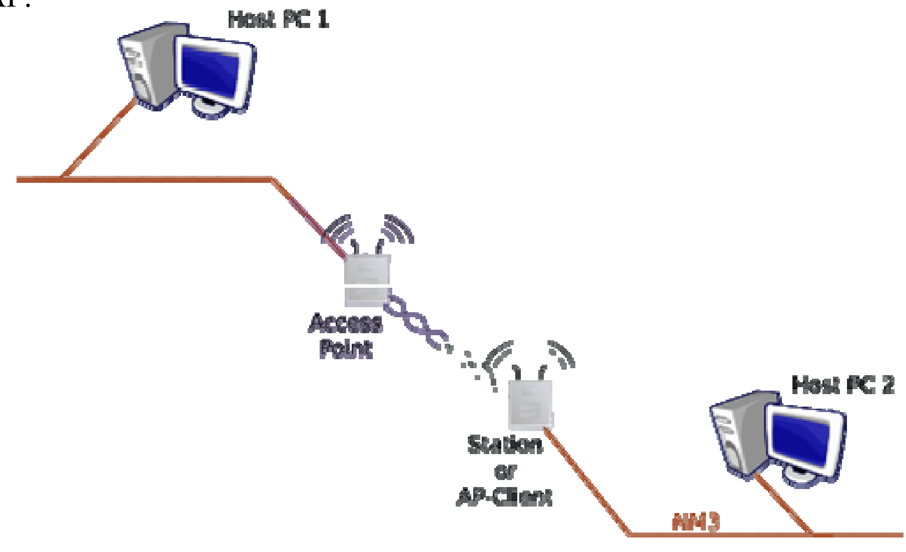


Figura 52. AP con cliente AP

El AP debería ser configurado como sigue:

1. Configurar el ESSID del AP.
2. Habilitar el modo sigiloso en el AP.
3. Habilitar una ACL para permitir y denegar los nodos clientes.

El cliente AP debería ser configurado como sigue:

1. Escriba el SSID del AP dentro Del campo SSID.
2. Escriba la dirección MAC del AP dentro del campo BSSID.
3. Otra opción es llevar a cabo un sondeo (site survey).
4. Seleccione el AP de la lista.
5. Haga todos los ajustes necesarios para optimizar el enlace.

5.5.2 Escenario Repetidor

El modo repetidor es un modo especial de NETKROM. La funcionalidad del modo repetidor se describe a continuación:

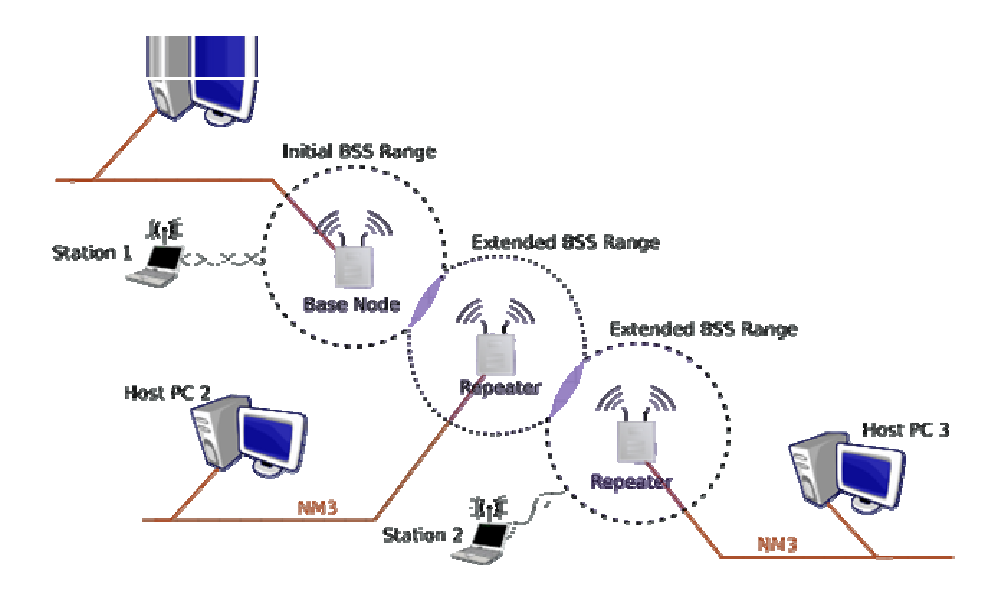


Figura 53. Topología del modo repetidor

En este escenario el nodo base de NETKROM es extendido a través del repetidor. Cada repetidor NETKROM expande el BSS del nodo anterior. Cada estación se conecta a un nodo repetidor diferente pero todos pertenecen al mismo BSS como si fuera el mismo AP. Esta topología es útil al crear una extensión grande de un nodo base AP. Además los repetidores ofrecen el puenteo de clientes inalámbricos con los clientes Ethernet de su interfaz Ethernet.

6. Enrutamiento Dinámico - RIP

Routing Information Protocol (RIP) es uno de los protocolos IGP (Interior Gateway Protocol) más usados en redes internas, el cual ayuda a los routers a adaptarse dinámicamente a los cambios de la red mediante el intercambio de información sobre qué redes cada router puede alcanzar y qué distancia están esas redes.

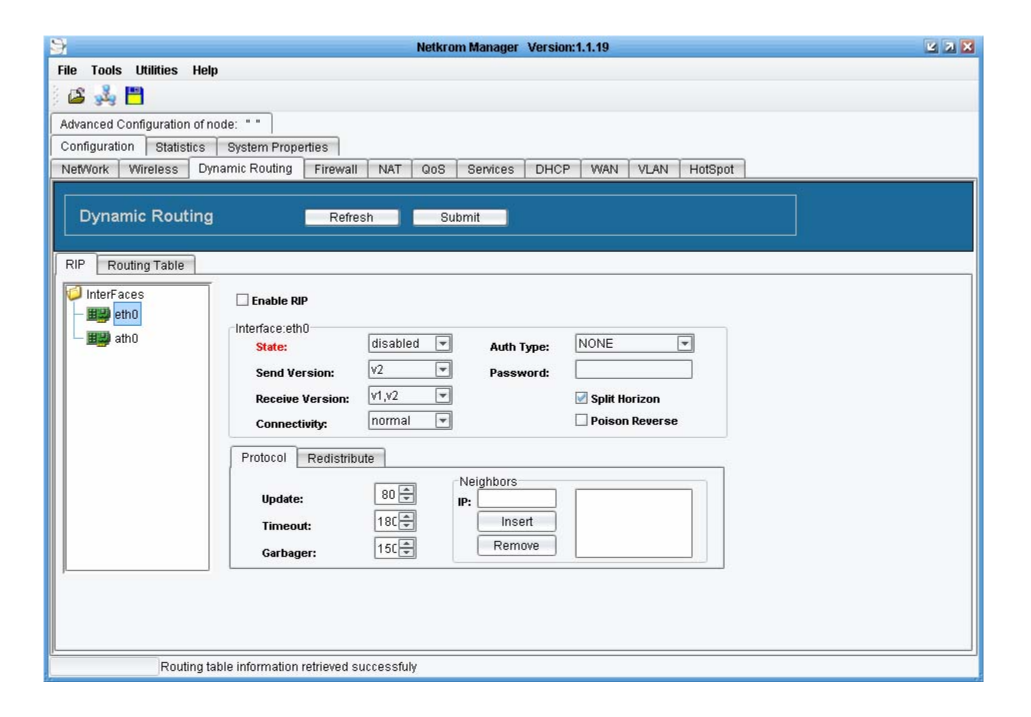
RIP es un protocolo de capa 3 del modelo de referencia OSI que usa el puerto 520 en UDP (User Datagram Protocol)

RIPv1

RIPv1, definido en el RFC 1058, usa enrutamiento con clase. Las actualizaciones de rutas no llevan información de la máscara. Además no soporta VLSM. Esta quiere decir que la sub redes en una red con clase deben ser del mismo tamaño. Tampoco soporta autenticación, haciéndolo vulnerable a varios ataques.

RIPv2

Debido a las deficiencias de RIPv1, RIPv2 fue desarrollado en 1994 e incluía la habilidad de llevar la información de la máscara y así soportar Classless Inter-Domain Routing (CIDR). Sin embargo para mantener la compatibilidad los 15 saltos como límite se mantuvo. Las actualizaciones de enrutamiento se envían como multicast 224.0.0.9 en contraposición a RIPv1 que envía actualizaciones como broadcast. Además de estas características RIPv2 soporta autenticación como MD5.



6.1 Parámetros Generales de RIP

- **Enable [Habilitar]:** Habilita el protocolo RIP.
- **State [Estado]:** Asigna el daemon de RIP a la interfaz seleccionada.
- **Send Version [Versión a Enviar]:** escoja la version de RIP a enviar.
- **Receive Version [Versión a Recibir]:** Selecciona la versión de RIP a recibir.
- **Connectivity [Conectividad]:** Selecciona el modo de operación del RIPd deamon, RIP clasifica a los routers como activos y pasivos. Los routers actives publican sus rutas a otros mientras que los routers pasivos escuchan y actualizan sus rutas basados en las publicaciones que reciben pero no publican sus tablas de enrutamiento. Típicamente los routers ejecutan RIP en modo activo mientras que los hosts en modo pasivo.
- **Auth Type [Tipo de Autenticación]:** solo disponible en RIPv2, permite a los paquetes ser autenticados a través de un password de texto no seguro o a través de MD5 basado en HMAC (keyed-Hashing for Message AuthentiCation). Habilitar la autenticación previene que las rutas sean actualizadas por otros routers no autenticados.
- **Password [Contraseña]:** contraseña.

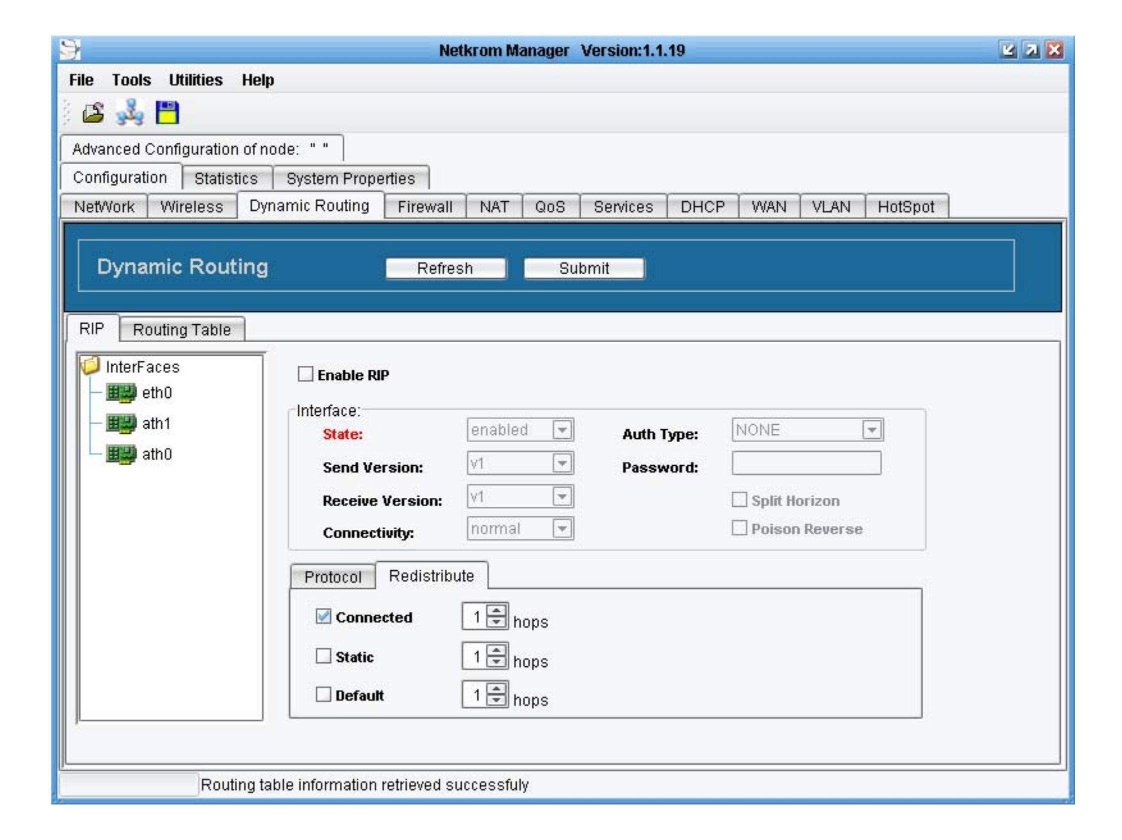
- **Split Horizon [Horizonte Dividido]:** habilita la opción de horizonte dividido. Esta regla consiste en no enviar actualizaciones de rutas aprendidas por las interfaces por las cuales las aprendió.
- **Poison Reverse [Envenenamiento en Reversa]:** Configura el horizonte dividido con la opción de envenenamiento en reversa. Es este caso las rutas aprendidas se envían por las interfaces por las cuales se aprendieron pero con una métrica de infinito (16 saltos).

6.2 Parámetros del Protocolo RIP

- **Update [Temporizador de Actualización]:** configura el temporizador de actualización, el router enviará sus actualizaciones cada vez que este temporizador venza.
- **Timeout [Temporizador de Expiración]:** configura el temporizador de expiración. Si un router no recibe una actualización para una ruta durante el temporizador de expiración, la ruta se la pone como inalcanzable es decir con una métrica d 16 pero no se elimina de la tabla de enrutamiento.
- **Garbager [Temporizador de Purga]:** Configura el temporizador de purga. Cuando una ruta sobrepasa el temporizador de purga se la elimina de la tabla de enrutamiento.
- **IP Neighbors [Vecinos IP]:** inserta o elimina las direcciones IP de los routers vecinos. Cuando un vecino no entiende los mensajes multicast, este comando es usado para especificar los vecinos. En algunos casos, no todos los routers serán capaces de entender los mensajes multicast, donde los paquetes se envían a un grupo de direcciones. En esta situación donde un vecino no puede procesar los paquetes multicast es necesario establecer un enlace directo entre los routers. Este campo le permite especificar la dirección IP del router vecino.

6.3 Parámetros de Redistribución RIP

- **Connected [Conectado]:** redistribuye las rutas conectadas dentro de la tabla RIP.
- **Static [Estática]:** redistribuye las rutas estáticas dentro de la tabla RIP.
- **Default [Por defecto]:** redistribuye las rutas por defecto dentro de la tabla RIP.



7. Firewall y NAT

Un firewall protege la red de ataques que podrían comprometer la confidencialidad, corrupción de datos y la denegación de servicios. Una red para que soporte la funcionalidad de firewall debe tener al menos dos interfaces de red, una para la red a proteger y la otra para la red que va a estar expuesta. El firewall se ubica en el medio de las dos redes usualmente entre una red privada y una red pública como internet.

Para configurar los parámetros de firewall, seleccione la pestaña **Firewall**, ubicado debajo de la pestañas **Advanced Configuration of Node [Configuración Avanzada del Nodo], Configuration [Configuración]**.

Para configurar los parámetros **NAT**, seleccione la pestaña **NAT**, ubicado debajo de **Advanced Configuration of Node [Configuración Avanzada del Nodo], Configuration [Configuración]**.

7.1 Firewall y NAT

NETKROM OS soporta características y funcionalidades avanzadas de firewall y NAT. Además cuenta con una administración y monitoreo fácil, suministrando una solución eficaz a los administradores de red.

7.1.1 Cadenas de Firewall

- **Input firewall [Firewall de Entrada]** - todo el tráfico entrante se compara con las reglas de firewall de entrada para ser aceptado.
- **Output firewall [Firewall de Salida]** - todo el tráfico saliente se compara con las reglas de firewall de salida para ser enviado.
- **Forwarding firewall** – Todo el tráfico es enviado a través del sistema operativo y se compara con las reglas de firewall de fordwarding para ser enviado.
- **Flowmark** - Todo el tráfico de entrada que concuerda con los criterios correspondientes es marcado.

7.1.2 Cadenas de NAT

- **DNAT** - Usado para alterar los atributos de destino del paquete (para re direccionarlos).

- **SNAT** - Usado para alterar los atributos de origen del paquete (para ocultar la dirección del remitente y sus propiedades).

La siguiente imagen muestra la manera en que los paquetes de datos fluyen a través de las cadenas de firewall y NAT:

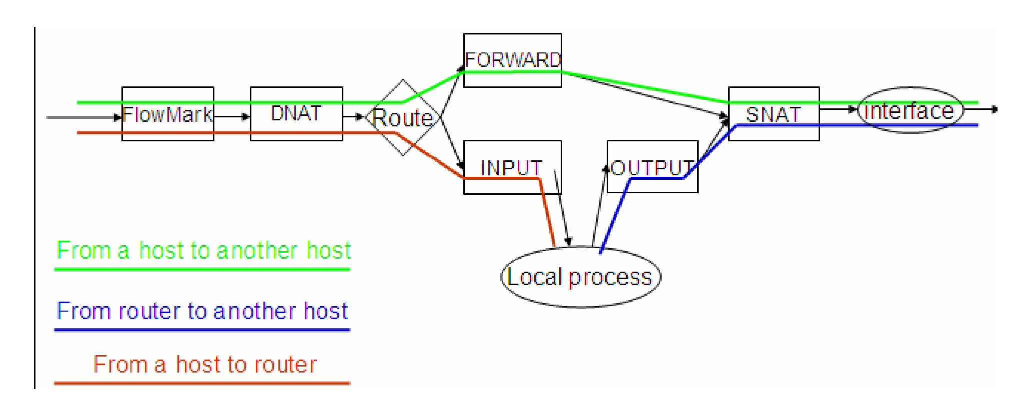


Figura 54. Diagrama del flujo de un paquete

7.2 Configurando Reglas del Firewall

Las reglas son entradas en una cadena las cuales consisten de varios campos (criterios) que pueden ser usadas para filtrar paquetes de datos. Si los criterios se cumplen, la regla concuerda y el paquete deja la cadena ejecutando la acción de la regla.

Desde la pestaña Firewall usted puede:

- seleccionar la cadena
- Configurar las políticas
- Agregar, eliminar y administrar reglas de Firewall
- Escribir reglas a la lista activa
- Refrescar la información mostrada

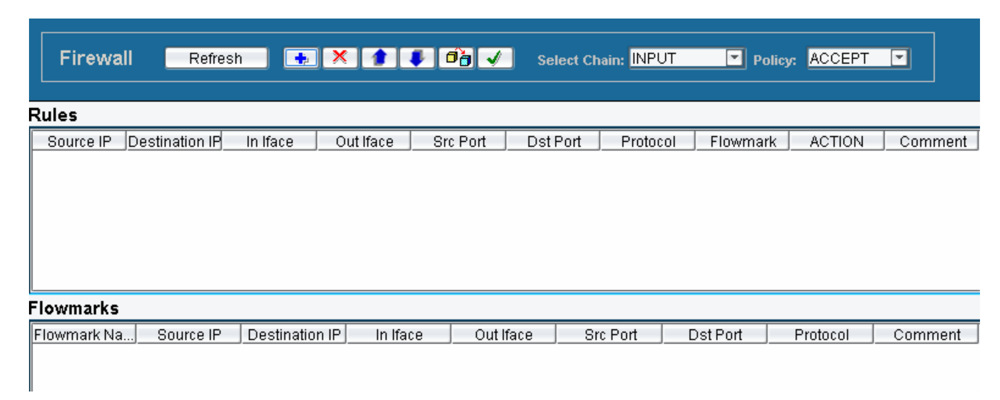


Figura 55. Cadenas de Firewall

Antes de configurar una regla, usted debe seleccionar **Select Chain [Seleccionar Cadena]** y configurar **Policy [Política].**

Seleccionar la Cadena

En la lista desplegable **Select Chain [Seleccionar cadena]**, seleccione **Input [Entrada]**, **Output [Salida] o Forward**.

Política

En la lista desplegable **Policy [Política]** seleccione entre **Accept [Aceptar]** o **Drop [Descartar].**

ACCEPT [Aceptar] - el paquete pasará a la siguiente cadena, dejando la cadena actual (ninguna regla más será examinada más adelante),

DROP [Descartar] – El paquete es descartado sin notificar al remitente.

7.2.1 Configuring Firewall Matching Fields

Click en el botón . El cuadro de diálogo de **Firewall Rule Configuration for [chain type] Chain** aparece. Este cuadro contiene dos pestañas: **Basic** y **Advanced.**

Casillas "Not"

En ambas pestañas, varios campos tienen una casilla **Not**. El campo Not invierte la operación de concordancia. Por ejemplo, **Source IP**: está configurado con una dirección IP específica. Cuando se marque la casilla la regla concordará con todos los paquetes excepto aquellos que tienen la dirección de orígenes especificados.

Configuración de Reglas Básicas

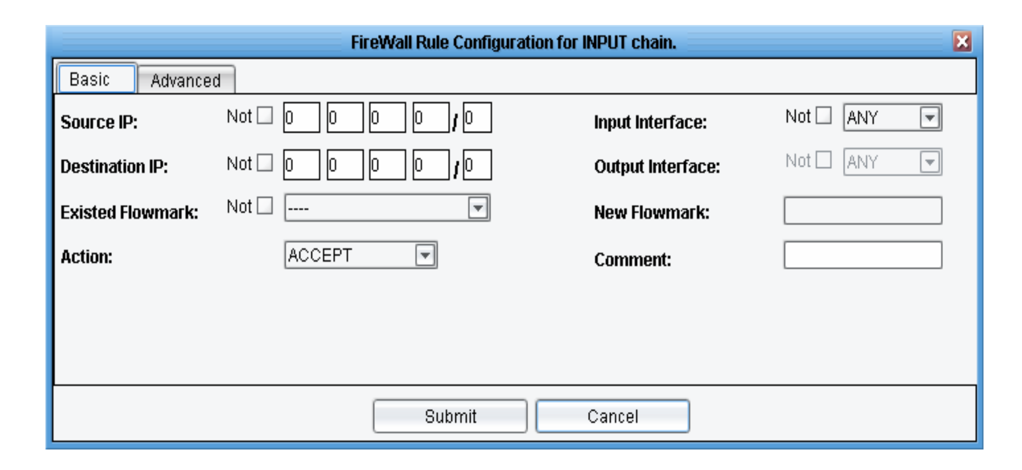


Figura56. Pestaña de configuración básica de las reglas de firewall

Source IP [Dirección IP de Origen]

Este campo muestra la dirección IP de origen del paquete. La dirección puede ser expresada como una dirección IP única (por ejemplo 192.168.1.1/32), o una red (Por ejemplo 192.168.1.0/24). Una concordancia ocurre si la dirección IP de origen del paquete es exactamente el mismo o pertenece a la red configurada. Escriba la dirección IP de origen y la máscara dentro del campo **Source IP**.

Destination IP [Dirección IP de Destino]

Este campo muestra la dirección IP de destino del paquete. La dirección puede ser expresada como una dirección IP única (por ejemplo 192.168.1.1/32), o una red (Por ejemplo 192.168.1.0/24). Una concordancia ocurre si la dirección IP de destino del paquete es exactamente el mismo o pertenece a la red configurada. Escriba la dirección IP de destino y la máscara dentro del campo **Destination IP**.

Input Interface [Interfaz de Entrada]

Este campo muestra la interfaz desde la cual se entregó el paquete. Una concordancia ocurre si la interfaz por el cual el paquete llegó es la misma que la interfaz configurada (si la interfaz configurada es un bridge, también concuerda con las interfaces debajo del bridge).

En la lista desplegable **Input Interface**, seleccione una interfaz, o seleccione **ANY**.

Output Interface [Interfaz de Salida]

Este campo muestra la interfaz desde la cual va a ser transmitido el paquete. Una concordancia ocurre si la interfaz por el cual el paquete va a ser transmitida es la misma que la interfaz configurada (si la interfaz configurada es un bridge, también concuerda con las interfaces debajo del bridge).

En la lista desplegable **Output Interface**, seleccione una interfaz, o seleccione **ANY**.

Flowmark Existente

Esta lista desplegable contiene los Flowmarks que ya han sido configurados. Seleccione un Flowmark desde la lista para configurar un Flowmark como una regla de concordancia de firewall. Una concordancia ocurre si el paquete fue marcado por esta marca cuando pasó a través de la cadena Flowmark.

Nuevo Flowmark

El campo **New Flowmark** está disponible si **Mark** está seleccionado en el campo A**ction**. Escriba el nombre del nuevo flowmark en el cuadro **New Flowmark.**

Action [Acción]

Cuando una regla concuerda, su acción se lleva a cabo. Estas acciones pueden ser:

ACCEPT [Aceptar] – el paquete pasará a la siguiente cadena, dejando la cadena actual en esta regla (ninguna regla será examinada después),

REJECT [Rechazar] – el paquete es descartado y envía un mensaje ICMP de inalcanzable al remitente.

DROP [Descartar] el paquete es descartado y no envía un mensaje ICMP de inalcanzable al remitente.
FORWARD - (actualmente no se usa)

MARK – El paquete pasará a la siguiente cadena, dejando la cadena actual en esta regla (ninguna regla será examinada después). Será marcado como **New Flowmark**.

Comment [Comentario]

Este campo es usado para ingresar una cadena de máximo 30 caracteres y así describir la regla.

Configuraciones Avanzadas de las Reglas

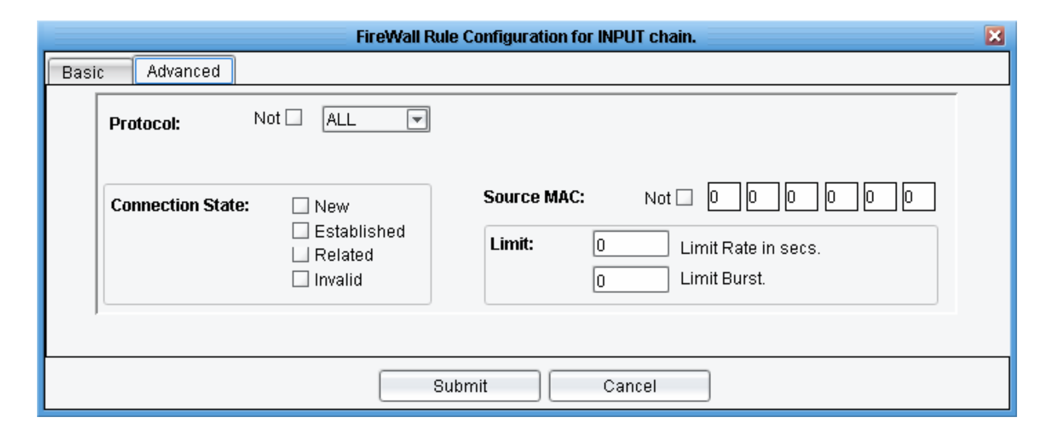


Figura 57. Configuración avanzada de las reglas de firewall

Protocol [Protocolo]

Esta lista desplegable contiene una lista de protocolos que pueden ser seleccionados para concordar. La ventana cambia de acuerdo al protocolo seleccionado. Los siguientes campos pueden ser configurados:

- **ALL [Todo] –** una concordancia siempre ocurre.
- **TCP** – una concordancia ocurre si
  1. el protocolo del paquete es **TCP**

2. El flag **SYN flag** del paquete concuerda basado en cual de lo siguiente está seleccionado en el flag de SYN:
   - ƒ **ALL** – siempre concuerda.
   - ƒ **SET** - una concordancia ocurre si el paquete empieza una nueva conexión.
   - ƒ **NOT SET** – una concordancia ocurre si el paquete es un miembro de una conexión empezada previamente.

3. **Source Port [Puerto de Origen]** el Puerto de origen se ingresa entre 0 y 65535 donde 0 indica que todos los puertos tienen que concordar.

4. **Destination Port [Puerto de destino]** el Puerto de destino se ingresa entre 0 y 65535 donde 0 indica que todos los puertos tienen que concordar.



Figura 58. Reglas de configuración avanzada TCP

- **UDP** – una concordancia ocurre si

5. El tipo de protocolo es **UDP**

6\. . **Source Port [Puerto de Origen]** el Puerto de origen se ingresa entre 0 y 65535 donde 0 indica que todos los puertos tienen que concordar.

7\. **Destination Port [Puerto de destino]** el Puerto de destino se ingresa entre 0 y 65535 donde 0 indica que todos los puertos tienen que concordar.

- **ICMP** – una concordancia ocurre si

8\. El tipo de protocolo es **ICMP**

9\. El tipo de **ICMP** concuerda basado en la siguiente lista:

1. **ANY**: una concordancia siempre ocurre
2. **REQUEST**: un a concordancia ocurre si es una petición ICMP.
3. **RESPONSE** un a concordancia ocurre si es una respuesta ICMP.

- **GRE** – una concordancia ocurre si el protocolo es **GRE** (Generic Routing Encapsulation)

- **ESP** - una concordancia ocurre si el protocolo es **ESP**
- **AH** – una concordancia ocurre si el protocolo es **AH**

Estado de la Conexión

NETKROM puede llevar a cabo funciones de firewall basado en el estado de la conexión. Las siguientes opciones se pueden configurar:

New – una concordancia ocurre si el paquete empieza una conexión nueva (el router ha visto paquetes en una dirección).

Established – una concordancia ocurre si un paquete es miembro de una conexión existente. (el router ha visto paquetes en ambas direcciones).

Related - una concordancia ocurre si el paquete empieza una conexión nueva, pero si también es un miembro de una conexión existente. (el router ha visto paquetes en ambas direcciones).

Invalid – una concordancia ocurre si el paquete no es miembro de una conexión existente peo si también no empieza una conexión nueva (paquete ambiguo).

Dirección MAC de Origen

Una concordancia ocurre si la dirección MAC del paquete (en el encabezado Ethernet) es la misma que la dirección en este campo. Escriba la dirección MAC en este campo.

Limit [Límite]

Este campo contiene configuraciones relacionadas al la velocidad a la cual el paquete llega.

Limit Rate – una concordancia ocurre si la velocidad configurada no se alcanza todavía.

Limit Burst – una concordancia ocurre si la velocidad burst no se ha alcanzado todavía.

Importante: *para habilitar una regla de firewall (escríbala dentro de la lista activa) usted debe hacer click en el botón que se muestra a la derecha.*



7.3 Configurando Reglas de NAT

Las reglas son entradas de una cadena que consisten de varios campos (criterios) que pueden ser usados para concordar un paquete. Si todos los criterios se cumplen, entonces la regla concuerda y el paquete deja la cadena, ejecutando la acción de la regla.

Desde la pestaña NAT usted puede:

- seleccionar el tipo de NAT
- Agregar, eliminar, editar y administrar las reglas NAT
- Escribir reglas NAT a las listas activas

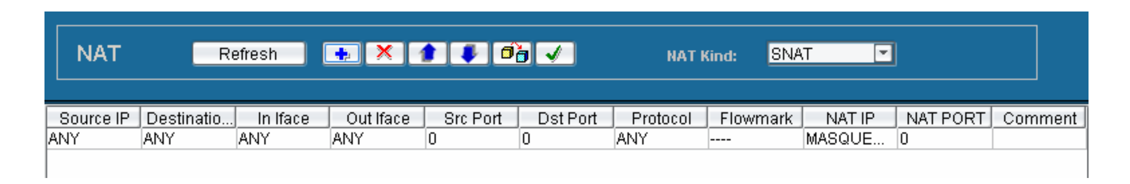


Figura 59. Cadenas NAT

Antes de configurar las reglas usted debe elegir el tipo de **NAT.**

NAT Kind

Seleccione entre **SNAT** o **DNAT.**

7.3.1 Configurando los Campos de Concordancia de NAT

Para agregar una regla, click en el botón  . Aparece el siguiente cuadro:

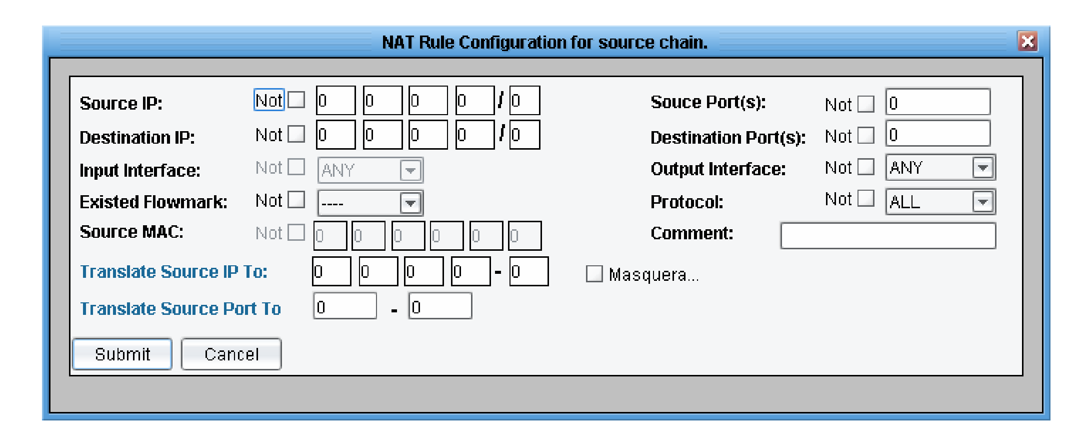


Figura 60. Configuración de las reglas de NAT

Campos Comunes de SNAT/DNAT

Los siguientes campos son comunes para SNAT y DNAT.

Not Check Boxes

Hay vario cuadros que dicen NOT. Estos campos invierten la operación de concordancia. Por ejemplo, **MAC de Origen**: es configurada con la dirección MAC específica. Cuando el NOT es seleccionado la concordancia ocurrirá con todos los paquetes que no tengan la dirección MAC especificada.

Source IP [Dirección IP de Origen]

Este campo muestra la dirección IP de origen del paquete. La dirección puede ser expresada como una dirección IP única (por ejemplo 192.168.1.1/32), o una red (Por ejemplo 192.168.1.0/24). Una concordancia ocurre si la dirección IP de origen del paquete es exactamente el mismo o pertenece a la red configurada. Escriba la dirección IP de origen y la máscara dentro del campo **Source IP**.

Destination IP

Este campo muestra la dirección IP de destino del paquete. La dirección puede ser expresada como una dirección IP única (por ejemplo 192.168.1.1/32), o una red (Por ejemplo 192.168.1.0/24). Una concordancia ocurre si la dirección IP de destino del paquete es exactamente el mismo o pertenece a la red configurada. Escriba la dirección IP de destino y la máscara dentro del campo **Destination IP**.

Source Port(s)

Este campo muestra el número del Puerto del nodo de origen. Una concordancia ocurre si el número de Puerto de origen es el mismo que el configurado en este campo.

Destination Port(s)

Este campo muestra el número del Puerto del nodo de destino. Una concordancia ocurre si el número de Puerto de destino es el mismo que el configurado en este campo.

Input Interface

Este campo muestra la interfaz desde la cual se entregó el paquete. Una concordancia ocurre si la interfaz por el cual el paquete llegó es la misma que la interfaz configurada (si la interfaz configurada es un bridge, también concuerda con las interfaces debajo del bridge).

En la lista desplegable **Input Interface**, seleccione una interfaz, o seleccione **ANY**.

Output Interface

Este campo muestra la interfaz desde la cual va a ser transmitido el paquete. Una concordancia ocurre si la interfaz por el cual el paquete va a ser transmitida es la misma que la interfaz configurada (si la interfaz configurada es un bridge, también concuerda con las interfaces debajo del bridge).

En la lista desplegable **Output Interface**, seleccione una interfaz, o seleccione **ANY**.

Existing Flowmark

Esta lista desplegable contiene los Flowmarks que ya han sido configurados. Seleccione un Flowmark desde la lista para configurar un Flowmark como una regla de concordancia de firewall. Una concordancia ocurre si el paquete fue marcado por esta marca cuando pasó a través de la cadena Flowmark.

Protocol

Contiene toda la lista de protocolos a concordar:

- **ALL –** una concordancia siempre ocurre.
- **TCP** una concordancia ocurre si el protocolo es TCP y

  10. **Source Port [Puerto de Origen]** el Puerto de origen se ingresa entre 0 y 65535 donde 0 indica que todos los puertos tienen que concordar.

  11. **Destination Port [Puerto de destino]** el Puerto de destino se ingresa entre 0 y 65535 donde 0 indica que todos los puertos tienen que concordar.

- **UDP** - una concordancia ocurre si el protocolo es UDP y,

  12. **Source Port [Puerto de Origen]** el Puerto de origen se ingresa entre 0 y 65535 donde 0 indica que todos los puertos tienen que concordar.
  13. **Destination Port [Puerto de destino]** el Puerto de destino se ingresa entre 0 y 65535 donde 0 indica que todos los puertos tienen que concordar.

- **ICMP –** una concordancia ocurre si el protocolo es ICMP
- **GRE -** una concordancia ocurre si el protocolo es GRE
- ***AH* -** una concordancia ocurre si el protocolo es AH
- ***ESP* -** una concordancia ocurre si el protocolo es ESP

Dirección MAC de Origen

Una concordancia ocurre si la dirección MAC del paquete (en el encabezado Ethernet) es la misma que la dirección en este campo. Escriba la dirección MAC en este campo.

Comment

Se usa para un comentario y así describir a la regla.

Campos Específicos de SNAT

Los siguientes campos solo están disponibles para SNAT.

Masquerade: la dirección IP que va a ser asignada a los paquetes salientes es dinámicamente almacenada (no se necesita configurar explícitamente la dirección IP de salida).

Translate Source IP to: la dirección IP (o rango de direcciones IP) a la cual la dirección de origen del paquete va a ser cambiado. En el caso de que sea un rango de direcciones, un algoritmo es usado para asignar las direcciones.

Translate Source Port to: el rango de los puertos del router que son usados para enviar paquetes y seguir sus respuestas.

Campos Específicos del DNAT

Los siguientes campos solo están disponibles para DNAT.

Redirect – cuando una concordancia ocurre, el paquete será direccionado al Puerto del router.

Translate Dest IP to – la dirección IP (o rango de direcciones IP) a la cual la dirección de origen del paquete va a ser cambiado. En el caso de que sea un rango de direcciones, un algoritmo es usado para asignar las direcciones. Esto es usado para enviar el paquete a otro host.

Translate Dest Port to – el puerto por el cual el paquete sera enviado (si es un rango de puertos se usa un algoritmo).

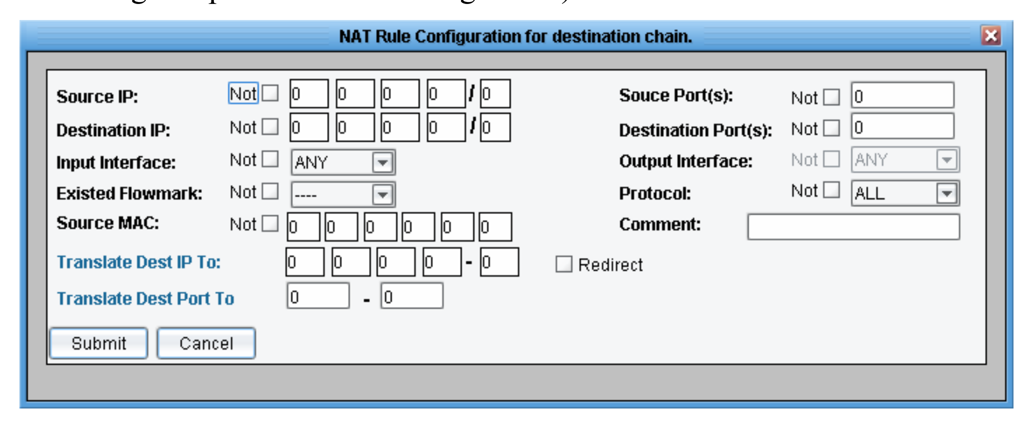


Figura 61. DNAT

Importante: *para habilitar una regla de NAT (escríbala en la lista activa) usted debe hacer click en el botón.*

7.3.2 Ejemplos

Los siguientes ejemplos son útiles para entender las reglas de NAT.

Denegar la Conexión SSH hacia su Router desde Internet.

SSH por defecto usa el puerto 22. Asuma que el router está conectado a internet a través de la interfaz eth0. Para deshabilitar las conexiones SSH desde internet, usted puede insertar una en la entrada de la cadena del firewall que descartará la conexión (ya que este protocolo usa TCP, el flag SYN estará activado).

Para llevar a cabo esto, configure las reglas de firewall como sigue:

En la pestaña Basic:

Source IP:	0.0.0.0/0 (cualquiera)
Destination IP:	0.0.0.0/0 (cualquiera)
Input interface:	eth0 (la conexión a internet)
Comment:	Denegar la conexión SSH desde Internet
ACTION:	DROP

En la pestaña Advanced:

Protocol:	TCP
SYN Flag:	SET
Source Port:	0 (Cualquiera)
Destination Port:	22 (SSH)

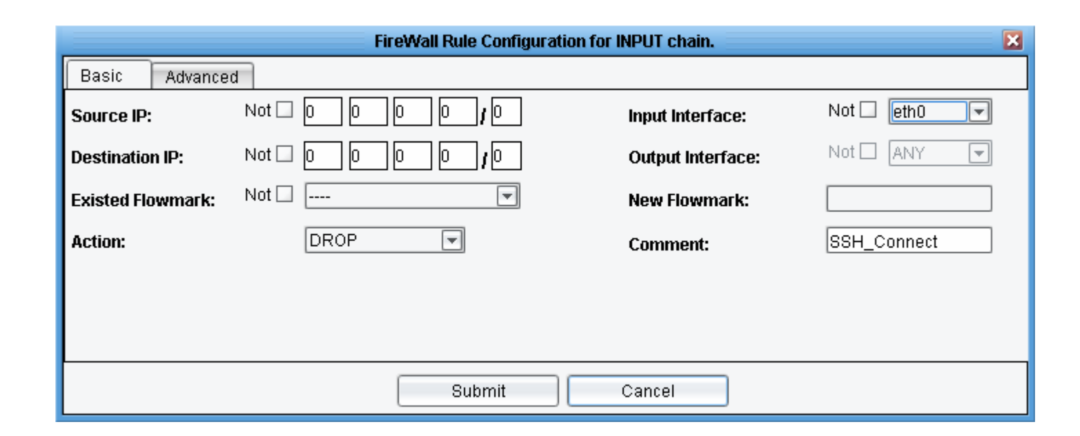


Figura 62. Pestaña básica del ejemplo

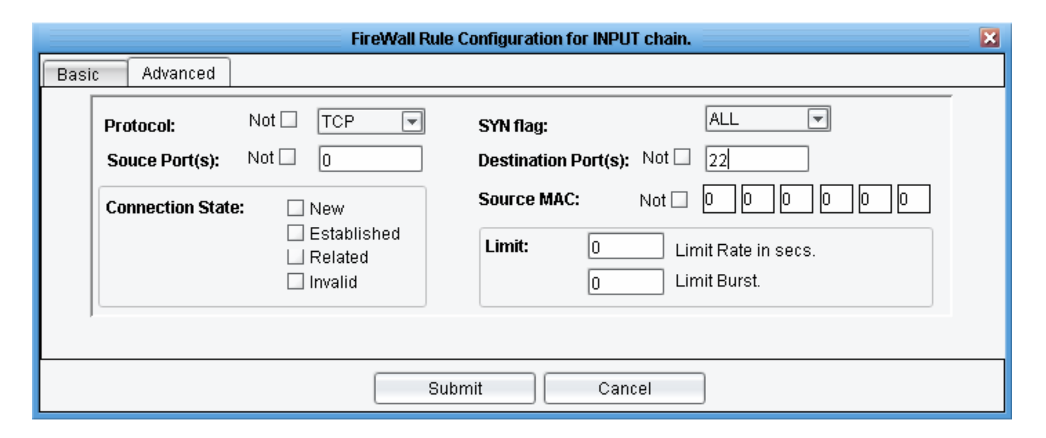


Figura 63. Pestaña avanzada del ejemplo

Click en **Submit** para agregarla a la lista y aplicarla al router.

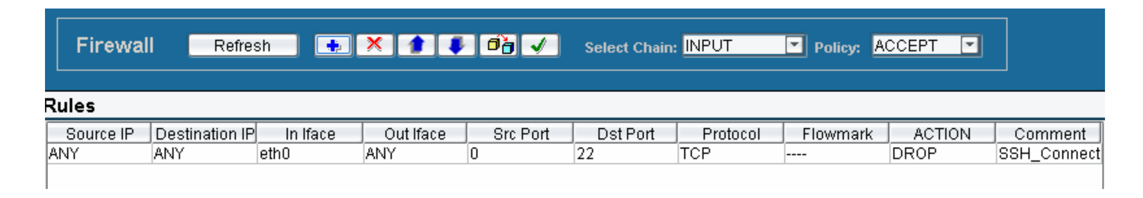


Figura 64. Ejemplo de firewall

NAT: Permitir el Acceso a Internet de una Red Privada usando solo una Dirección IP Pública.

Asuma que el router está conectado a internet a través de la interfaz eth0 y su dirección IP es 173.55.1.2/24. Su red local está conectada a la interfaz eth1 con dirección IP 192.168.1.1/24. Usted debería traducir todo el tráfico de salida a internet (interfaz eth0) originado desde su red local (interfaz eth1).

Inserte una regla a la cadena SNAT como sigue:

Detalles

Source IP: 192.168.1.0/24 (Red local)

Output Interface: eth0

Translate Source IP to: 173.55.1.2 MASQUERADE (dirección IP de la interfaz eth0)

Comment: NAT_en_WAN

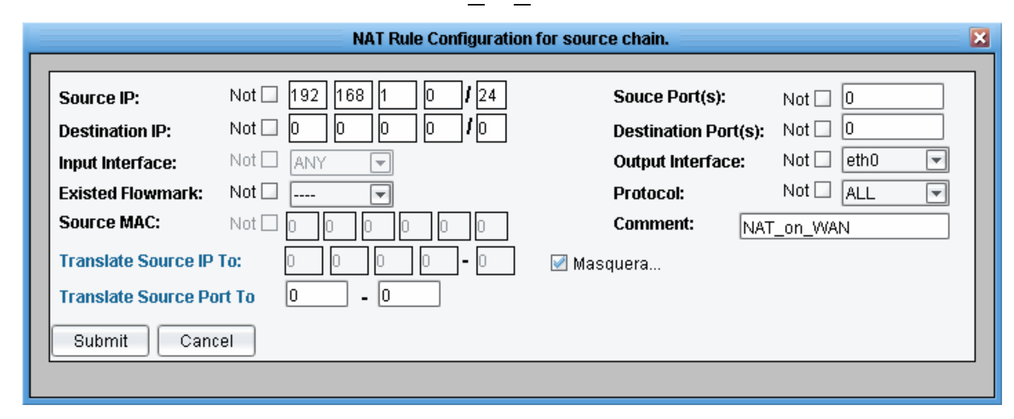


Figura 65. Ejemplo de configuración de NAT

Click en **Submit** para agregarla a la lista y aplicarla al router.

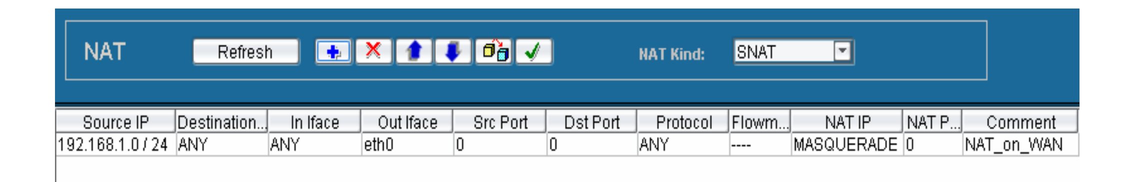


Figure 66. *Ejemplo de NAT*

Importante: Asegúrese que el IP Forwarding esté habilitado en el router.

Importante: Para habilitar la regla NAT (escríbala en la lista activa) usted debe hacer click en el botón ✓.

8. DHCP

El protocolo **Dynamic Host Configuration Protocol (DHCP)** suministra parámetros de configuración a los hosts en un modelo cliente servidor.

DHCP consiste de dos componentes: un protocolo que entrega parámetros de configuración específicos desde un servidor a los hosts y un mecanismo para la asignación de direcciones a los hosts.

Para configurar parámetros **DHCP**, seleccione la pestaña **DHCP**, ubicada debajo de las pestañas **Advanced Configuration of Node, Configuration**. La pestaña DHCP contiene dos sub pestañas: **Server** y **Client**.

8.1 Configurando un Servidor DHCP

El servidor NETKROM DHCP suministra una gran cantidad de parámetros para su configuración.

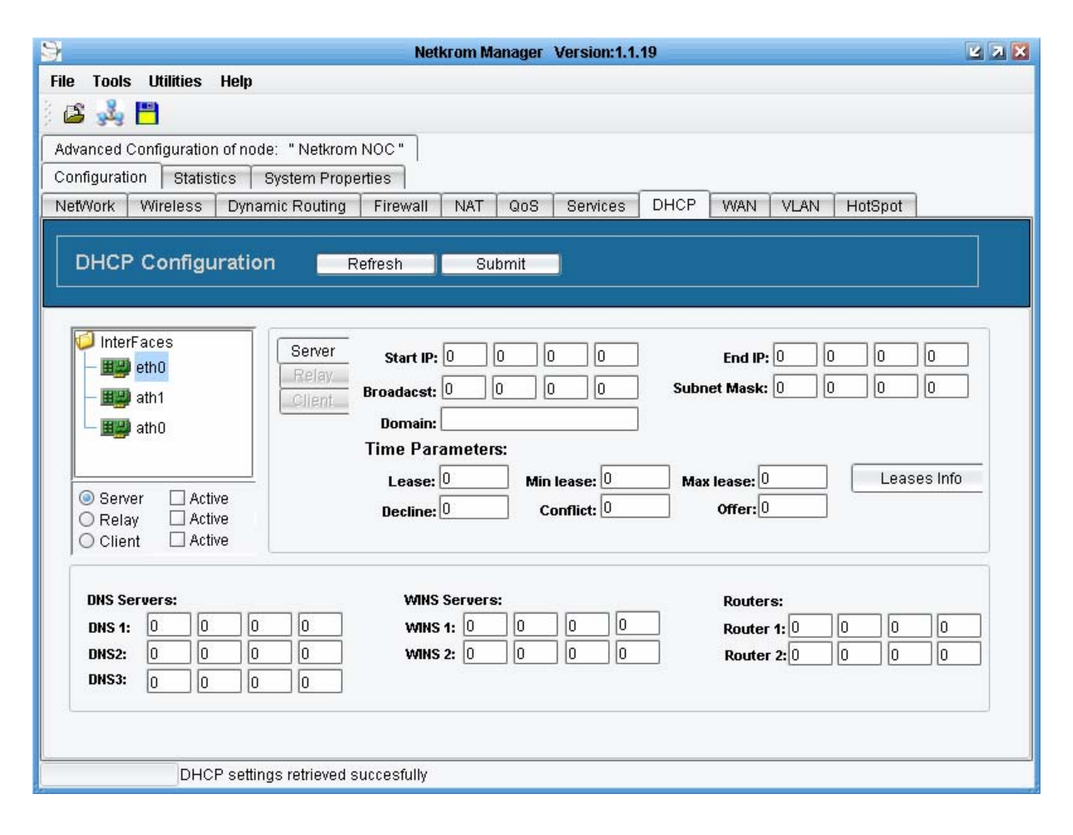


Figura 67. Configuración de un servidor DHCP

Para configurar un servidor **DHCP**, seleccione la interfaz desde el árbol de interfaces. Solo los clientes en la misma interfaz física serán capaces de adquirir direcciones IP desde el servidor DHCP. Si los clientes de otra interfaz física deben adquirir direcciones IP desde el mismo servidor, un bridge debe ser creado y las interfaces deben ser agregadas al bridge. Después seleccione el bridge como la interfaz para el servidor DHCP.

NOTA: *Usted no puede seleccionar una interfaz que pertenezca a un bridge como la interfaz para el servidor DHCP. Adicionalmente la interfaz del servidor DHCP debería haber sido ya configurada con una dirección IP y máscara de subred. Múltiples servidores DHCP en diferentes interfaces también está permitido.*

8.1.1 Configurando los Campos del Servidor DHCP

Para configurar los parámetros del servidor DHCP, seleccione el botón **Server [Servidor]** y luego marque la casilla **Active [Activo]**. La pestaña **Server [Servidor]** se habilita.

Después de llenar los campos requeridos, click en el botón **Submit [Enviar]** para cargar la configuración al nodo sin empezar el servidor.

Start IP [IP de inicio] y End IP [IP final]

Escriba el rango de direcciones IP en los campos **Start IP** y **End IP**. Estas direcciones son el límite para el pool de direcciones del servidor DHCP.

Broadcast

Escriba la dirección IP apropiada dentro del campo **Broadcast**. Este campo contiene la dirección IP que los clientes usarán. La dirección IP de Broadcast debería ser una de las direcciones que la máscara de sub red permita.

Subnet Mask [Máscara de subred]

Escriba la máscara de subred en el campo **Subnet**. Esta es la máscara de subred que los clientes usarán.

Domain [Dominio]

Escriba el nombre del dominio (si hay alguno) dentro del campo **Domain** que será asignado a los clientes.

Time Parameters [Parámetros de tiempo]

Para cada uno de los siguientes campos, escriba el valor apropiado dentro del recuadro.

Lease [Arrendamiento]

Este campo contiene el número de segundos que una dirección IP asignada es válida. Después de la expiración el cliente tiene que renegociar para conseguir una nueva dirección IP (la cual es usualmente la misma). El tiempo de expiración se configura en este campo.

Decline [Declinación]

Este campo contiene el número de segundos que una dirección IP será reservada o arrendada si un mensaje de declinación es recibido.

Min Lease [Mínimo Arrendamiento]

Este campo contiene el mínimo valor en segundos. si un arrendamiento que se va a dar tiene un valor menor que este valor, se usa el tiempo de arrendamiento.

Conflict [Conflicto]

Este campo contiene la cantidad de tiempo (segundos) que una dirección IP va a ser reservada (arrendada) s i un conflicto ARP (dos clientes con la misma dirección IP) ocurre.

Max Lease [Máximo Arrendamiento]

Este campo contiene el número máximo de arrendamientos actuales (direcciones IP asignadas). Después de que se alcanza este límite, el servidor para de asignar direcciones IP a los clientes nuevos.

Offer

Este campo contiene el número de segundos que una dirección IP ofrecida se reserva. Este campo especifica el número de segundos que el servidor DHCP debería esconder las ofertas. El valor por defecto es 60 segundos. En redes rápidas, este valor puede disminuirse.

DNS Servers [Servidores DNS]

Escriba las direcciones IP de los DNS que los clientes usarán.

WINS Servers

Si hay servidores WINS que los clientes deberían usar, escriba las direcciones de los servidores WINS en los campos (WINS 1 y WINS 2).

Routers

En los campos Router 1 y Router 2, escriba las direcciones IP de las puertas de enlaces predeterminadas que los clientes usarán.

Leases Info [Información de arrendamiento]

Click en este botón para ver un cuadro de todas las direcciones IP asignadas por el servidor DHCP.

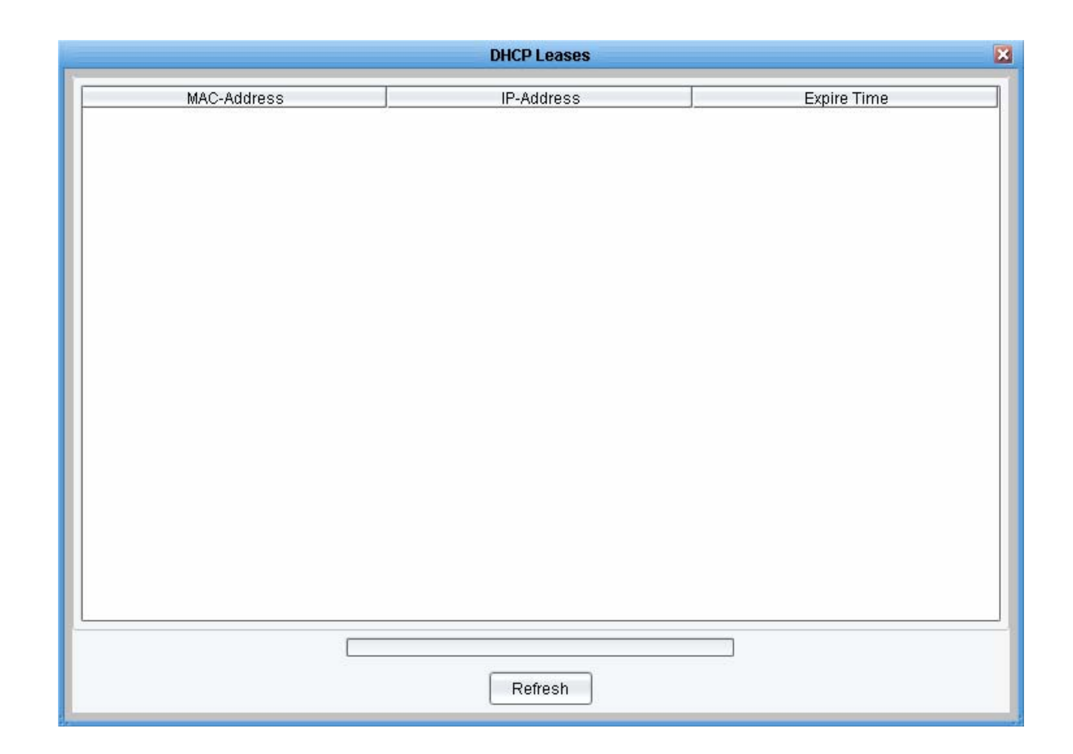


Figura 68. Cuadro de direcciones IP asignadas por el servidor DHCP

En la version actual del servidor DHCP la configuración no soporta cambios dinámicos de los arrendamientos DHCP. Después de una asignación IP usted es capaz de ver la nueva grabación en el cuadro de arriba después de aproximadamente 60 segundos de retraso.

8.1.2 Estrategias del tiempo de arrendamiento

Una de las preguntas más comunes de la administración de DHCP es, “que configuración debería dar a los tiempos de arrendamiento” así como en muchas preguntas sobre redes, “depende”. El criterio de decisión primaria es la frecuencia a la cual sus clientes la configuración de sus datos.

Si usted está usando DHCP solo para asignar direcciones de forma aleatoria, tener tiempos de arrendamientos grandes resultará en un mayor nivel de estabilidad. Por ejemplo, si usted usa un tiempo de arrendamiento de un mes o más, un corte temporario es probable que no afecte sus operaciones normales. Sin embargo, si usted está usando DHCP con una gran cantidad de configuraciones (como por ejemplo los servidores DNS), usted deseará tener un periodo de arrendamiento menor para que los cambios en la red sean reconocidos rápidamente por los clientes DHCP. En este caso, tener tiempos de arrendamiento mayores a un día o dos pueden ser problemáticos ya que los clientes que obtienen un nuevo arrendamiento antes de un cambio crítico en la red no reconocerán este cambio hasta que el tiempo de arrendamiento expire o sea renovado.

8.2 Configurando un Cliente DHCP

La configuración de un cliente DHCP es simple. El único requisito es seleccionar la interfaz donde el cliente DHCP buscará por servidores DHCP.

Similar a la configuración del servidor DHCP, múltiples instancias de clientes DHCP en diferentes interfaces está permitido.

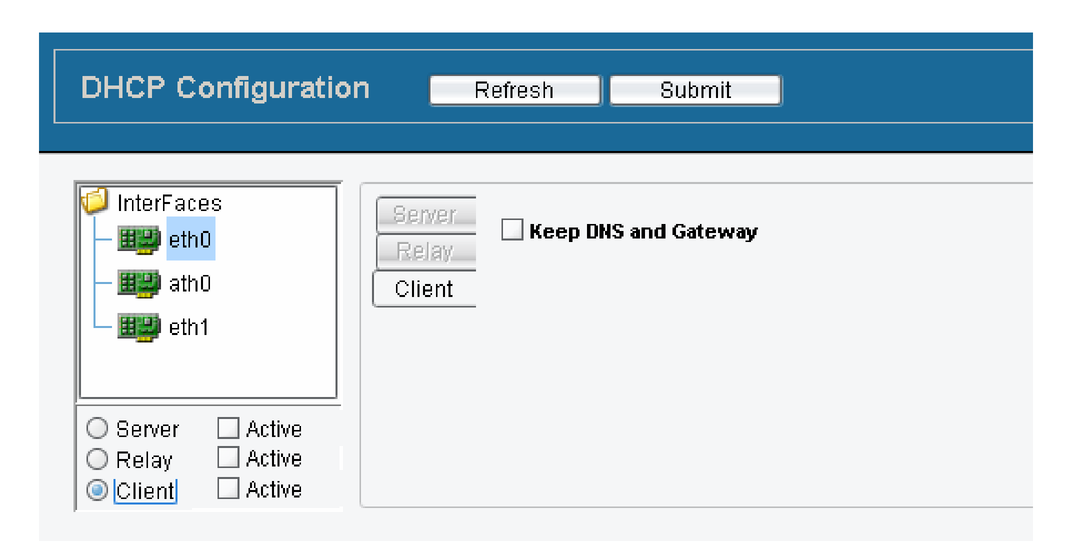


Figura 69. Cliente DHCP

Para configurar un cliente DHCP seleccione la interfaz del árbol de interfaces.

Para configurar los parámetros del cliente DHCP, seleccione el botón **Client [Cliente]** y seleccione la casilla **Active [Activo]**. La pestaña **Client [Cliente]** se habilita.

Para prevenir los cambios de gateway y DNS del cliente cuando el cliente recibe una dirección IP del servidor, seleccione la casilla **Keep DNS and Gateway [Mantener Gateway y DNS]**. Esto es útil cuando usted ya ha configurado un gateway y los DNS y no quiere que cambien o si estos parámetros son configurados por otra aplicación (por ejemplo cliente PPPoE). En otros muchos casos este campo debería no seleccionarse.

Para completar la configuración click en el botón S**ubmit [Enviar].**

8.3 Configurando un DHCP Relay

DHCP no requiere un servidor en cada subred. Para ello se configure un DHCP Relay el cual escucha las peticiones DHCP y las envía a una dirección IP específica (el cual se encuentre en otro segmento de red). Esto elimina la necesidad de tener un servidor DHCP en cada red.

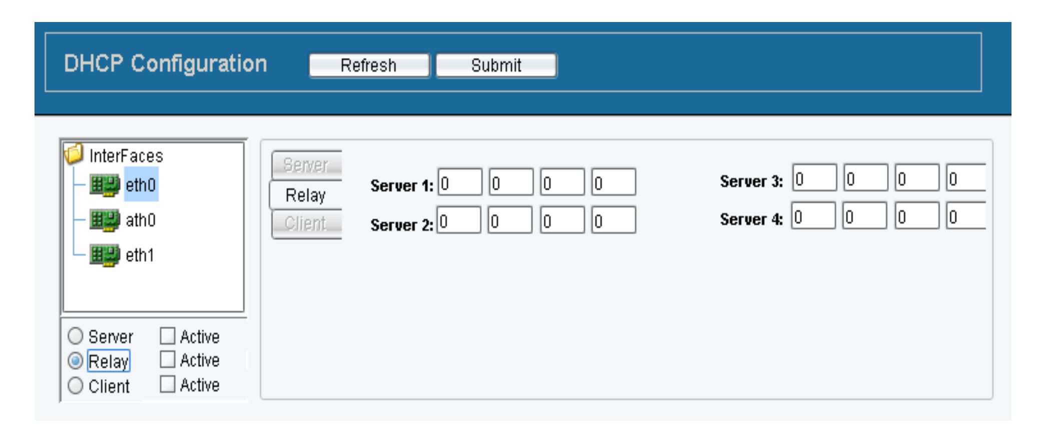


Figura 70. DHCP Relay

Para configurar un **DHCP Relay**, seleccione la interfaz del árbol de interfaces.

Para ver el panel complete de **DHCP Relay**, seleccione el botón **Relay**, luego marque la casilla **Active [Activo]**. El panel de configuración de DHCP Relay aparece.

Escriba la dirección IP a la cual las solicitudes de DHCP serán redirigidas en los campos Server 1, Server 2, Server 3, Server 4.

El DHCP Relay puede ser configurado en cada interfaz.

Para completar la configuración haga click en el botón **Submit [Enviar].**

9. WAN

Para configurar los parámetros **WAN**, seleccione la pestaña **WAN**, ubicada debajo de las pestañas **Advanced Configuration of Node, Configuration**. La pestaña WAN contiene dos sub pestañas: **PPPoE** y **PPTP**.

9.1 Configurando un Cliente PPPoE

La aplicación de cliente PPPoE es usada para crear conexiones PPPoE con servidores PPPoE y es usado principalmente por proveedores de servicios de internet.

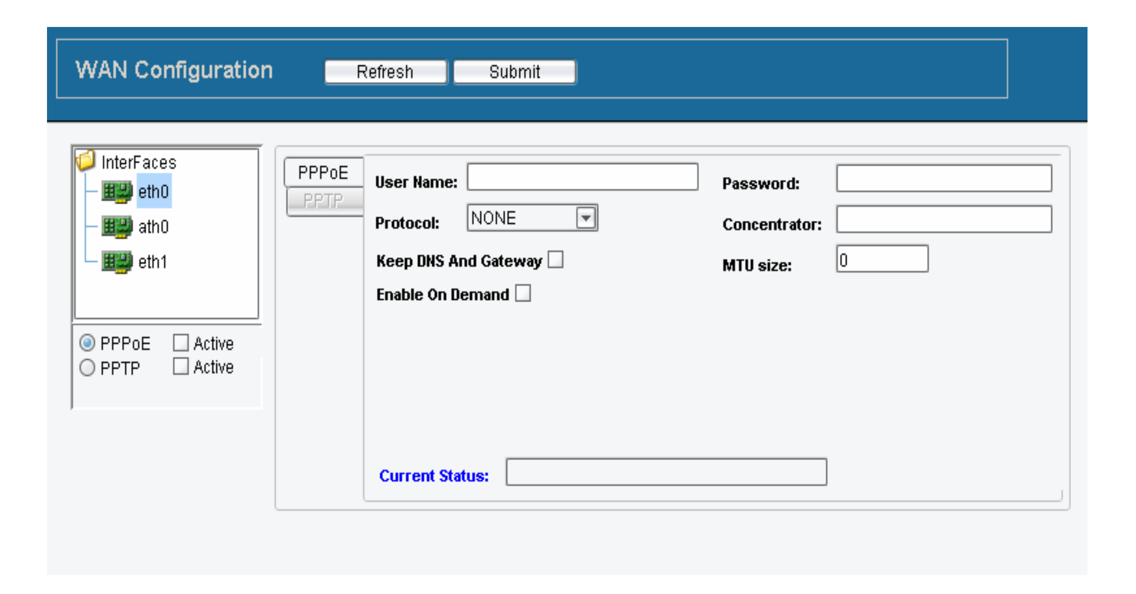


Figura 71. Configuración PPPoE

Para configurar un cliente PPPoE, seleccione la interfaz desde el árbol de interfaces. Esta interfaz usualmente comparte el mismo medio con un módem ADSL (en modo bridge). No es necesario tener pre configurada una dirección IP y máscara en la interfaz.

Para configurar un cliente PPPoE, seleccione el botón **PPPoE** y active la casilla **Active [Activo]**. El panel PPPoE aparece.

Después de llenar los campos requeridos haga click en el botón **Submit [Enviar].**

9.1.1 Configurando los Campos de Cliente PPPoE

User Name [Nombre de usuario]

Escriba el nombre de usuario para el cliente que va a ser usado para autenticarse con el servidor PPPoE (usualmente es suministrado por el ISP).

Password [Contraseña]

Escriba una contraseña (más de tres carácteres) para el cliente. Esto es usado para autenticarse con el servidor PPPoE y usualmente es suministrado por el ISP.

Protocol [Protocolo]

En esta lista desplegable, seleccione el protocolo que va a ser usado para la autenticación con el servidor PPPoE. Los protocolos que se pueden seleccionar son: **None, PAP** y **CHAP**.

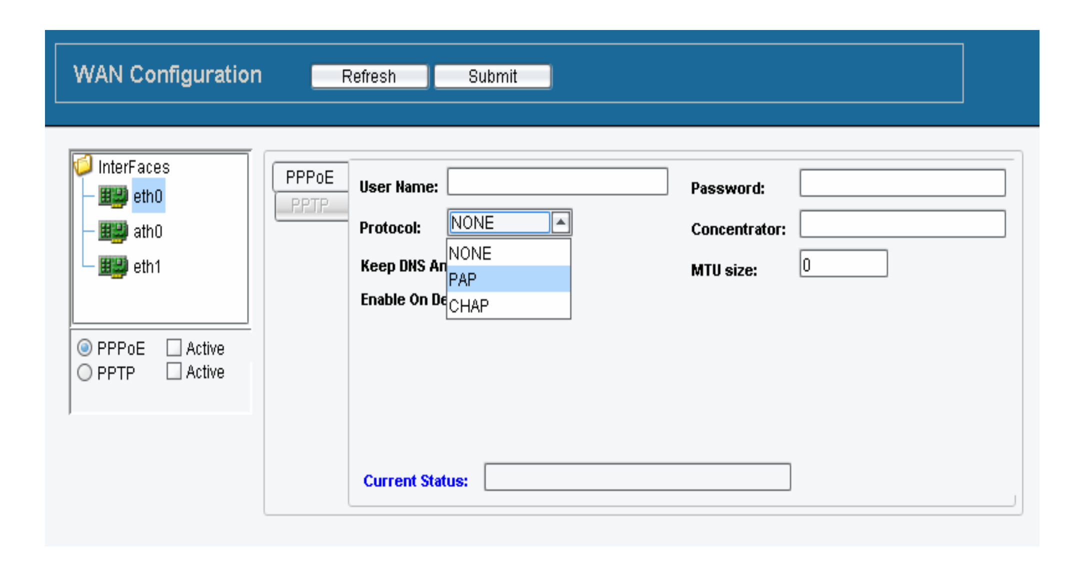


Figura 72. Configuración de PPPoE

Concentrator [Concentrador]

El concentrador contiene el nombre del servidor y se refiere al caso donde hay múltiples servidores PPPoE disponibles. Si esos servidores tienen un nombre importante (llamado nombre concentrador) usted puede elegir el apropiado escribiendo el nombre en este campo.

Keep DNS y Gateway

En muchos casos la autenticación PPPoE suministra al cliente con algunas direcciones DNS y hace la interfaz PPPoE la puerta de enlace predeterminada. Para configurar una dirección DNS y un gateway o dejar que otra aplicación los configure (por ejemplo un cliente DHCP), seleccione la casilla **Keep DNS and Gateway [Mantener DNS y Gateway]**.

MTU size [Tamaño del MTU]

El tamaño normal del MTU de Ethernet es de 1500 bytes, pero el encabezado PPPoE suma dos bytes de encabezado a la trama PPP encapsulada, esto significa que el MTU de la interfaz PPP es más de 1492 bytes. Esto causa todo tipo de problemas si usted está usando un computador con Linux como un firewall y las interfaces detrás del firewall tienen un MTU mayor de 1492. Por seguridad el tamaño del MTU debe ser un número entero entre 536 y 1412.

Enable on Demand [Habilitar cuando hay Demanda]

Enable on Demand es una característica la cual habilita la funcionalidad de crear una conexión PPPoE solo cuando hay tráfico IP en la interfaz PPPoE. Algunos ISPs ofrecen acuerdos de conexión donde el cobro depende del tiempo. En estos casos esta característica podría ser muy importante. Cuando **Enable on Demand** está seleccionado, los siguientes campos aparecen: **Remote Domain [Dominio Remoto], Remote IP [IP Remoto]** y **Demand Time [Tiempo de demanda]**

Para configurar este campo identifique el servidor PPPoE por su dirección IP y escriba la dirección dentro del campo **Remote IP**, o determine su nombre de dominio y escríbalo dentro del campo **Remote Domain**. Luego escriba un periodo de tiempo (en segundos) dentro del campo **Demand Time**. Si una conexión PPPoE permanece inactive durante este periodo, la conexión se cierra hasta que usted intente usar esto de nuevo (probablemente desde una PC detrás del router).

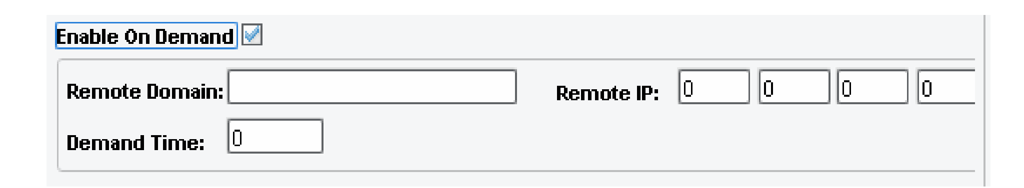


Figura 73. Habilitar el PPPoE cuando hay demanda

Current Status [Estado Actual]

Cuando usted hace click en el botón Refresh el campo **Current Status** muestra información de la conexión actual (si hay una conexión o la razón de un intento no exitoso para conectarse).

9.2 Configurando un Cliente PPTP

La aplicación de cliente PPTP es usada para crear conexiones PPTP con los servidores PPTP y es principalmente usado por ISPs.

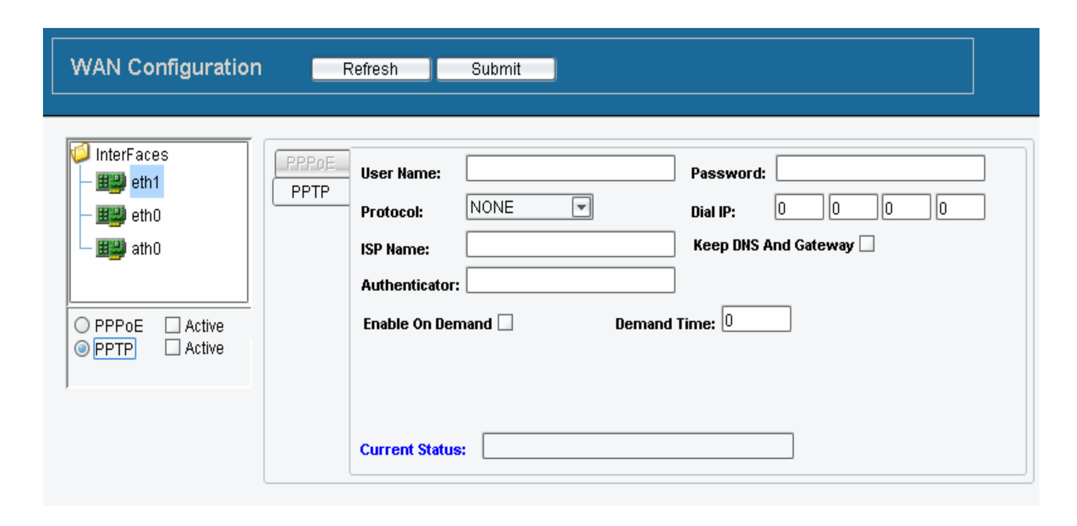


Figura 74. Configuración WAN - PPTP

Para configurar un cliente **PPTP**, seleccione la interfaz desde el árbol de interfaces. El fondo se torna azul. Esta interfaz debe ser pre configurada con una dirección IP válida y una máscara de red desde el servidor PPTP de alguna forma (por ejemplo a través de la puerta de enlace predeterminada).

Para ver el panel complete de la pestaña PPTP, seleccione el botón PPTP y marque la casilla **Active [Activo]**. El panel **PPTP** aparece.

Después de llenar los campos requeridos haga click en el botón **Submit [Enviar].**

9.2.1 Configurando los Campos de un Cliente PPTP

User Name [Nombre de usuario]

Escriba el nombre de usuario para el cliente que será usado para autenticarse con el servidor PPTP (usualmente proporcionado por el ISP).

Password [Contraseña]

Escriba una contraseña (más de tres carácteres) para el cliente. Esto es usado para autenticarse con el servidor PPTP y es usualmente proporcionado por el ISP.

Protocol [Protocolo]

En esta lista desplegable, seleccione el protocolo que va a ser usado para la autenticación con el servidor PPTP. Los protocolos son: **None, PAP** y **CHAP**.

Dial IP [Marcación IP] o ISP Name [Nombre del ISP]

Para identificar el servidor PPTP, escriba la dirección IP en el campo **Dial IP**, o escriba el nombre del DNS del servicio PPTP en el campo **ISP Name**.

Keep DNS [Mantener DNS] y Gateway

En muchos casos la autenticación PPTP proporciona al cliente una dirección DNS y hace que la interfaz del PPTP sea el gateway. Para configurar y una dirección DNS estática y una puerta de enlace predeterminada o dejar que otra aplicación los configure (por ejemplo un cliente DHCP) marque la casilla **Keep DNS and Gateway**.

Authenticator [Autenticador]

Algunos servidores PPTP requieren un autenticador para establecer una conexión PPTP. Este nombre es proporcionado usualmente por los ISPs.

Enable on Demand [Habilitar en demanda]

Esta característica habilita la funcionalidad de crear una conexión PPTP solo cuando hay tráfico IP en la interfaz PPTP. Algunos ISPs ofrecen acuerdos de conexión donde el cobro depende del tiempo. En estos casos esta característica podría ser muy valiosa.

Seleccione la casilla **Enable on Demand**, luego escriba un periodo de tiempo (segundos) dentro del campo **Demand Time**. Si una conexión PPTP no se usa por este periodo, la conexión se cierra hasta que usted intente usarlo de Nuevo (probablemente desde una PC detrás del router).

Current Status [Estado Actual]

Cuando usted hace click en el botón Refresh el campo **Current Status** muestra información actual de la conexión (si hay una conexión o la razón por un intento no exitoso para conectarse).

10. Calidad de Servicio

La calidad de servicio se refiere al concepto general de priorizar el tráfico de red de acuerdo a algunas de sus propiedades. Por defecto cada paquete es tratado igualmente. Sin embargo al utilizar QoS, ciertos patrones de tráfico de red se les pueden dar una prioridad mayor. Desde aquí en adelante, se referirá al patrón de tráfico como clase.

Algunas de las políticas que pueden ser mejorados con QoS son:

- Restringir o eliminar el ancho de banda consumido por aplicaciones P2P.
- Distribuir el ancho de banda disponible igualmente entre un grupo de usuarios de HOTSPOT.
- Asegurarse que ciertos servicios (por ejemplo el portal web de un hotspot) esté siempre accesible no importando cuanto de carga tenga la red.
- Reservar una porción del ancho de banda disponible para aplicaciones sensible a la latencia como por ejemplo VoIP.
- Mitigar ataques DoS mediante la restricción del uso de la red para tipos específicos de tráfico (por ejemplo tráfico ICMP).

10.1 La Pestaña QoS

Veamos primero, una vista rápida del GUI de QoS (Figura 77).

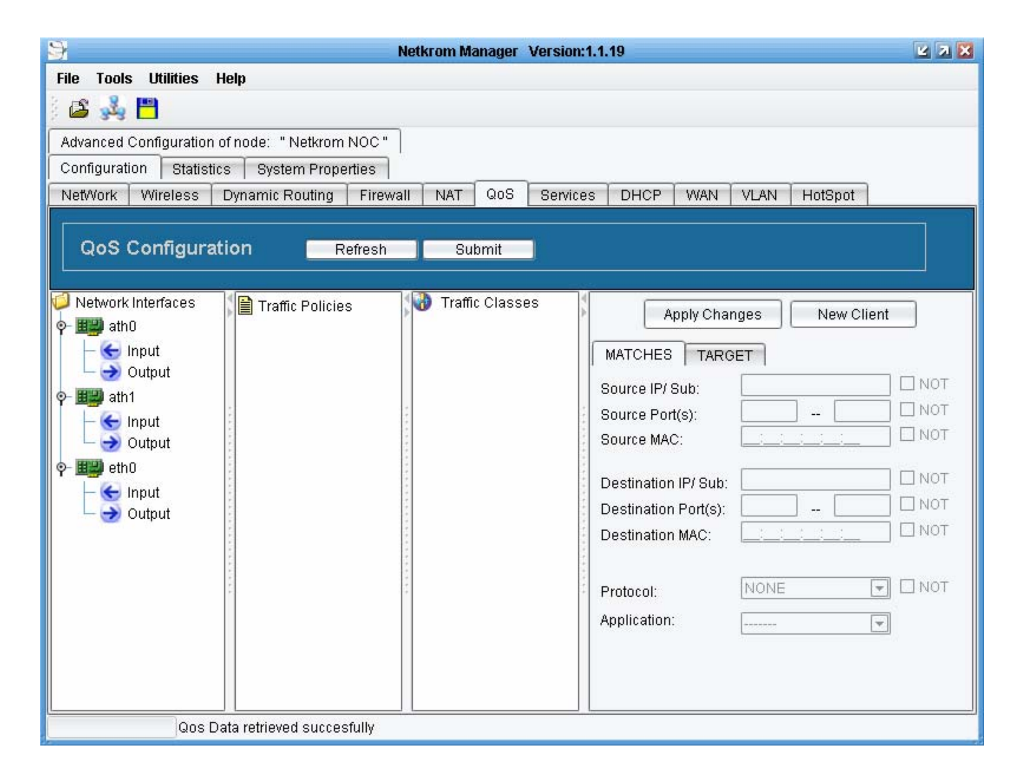


Figura 75. La ventana de QoS

Hay tres columnas principales:

10.1.1 Clases de Tráfico

Las clases de tráfico son entidades que se asocian a patrones de tráficos específicos y recursos de red específicos. El patrón de tráficos constituye las concordancias (*Matches*) asociados a una clase de tráfico y el recurso de red reservado, comprende el objetivo del tráfico de clase. Estas propiedades pueden ser configuradas vía el panel más a la derecha de la ventana QoS.

Para agregar una clase de tráfico nueva, usted tiene que hacer click derecho en la etiqueta "Traffic Classes" en el respectivo panel. Usted puede definir tantas clases de tráfico como usted lo desee. Una clase de tráfico puede también formar parte de un árbol jerárquico de sub clases (figura 78).

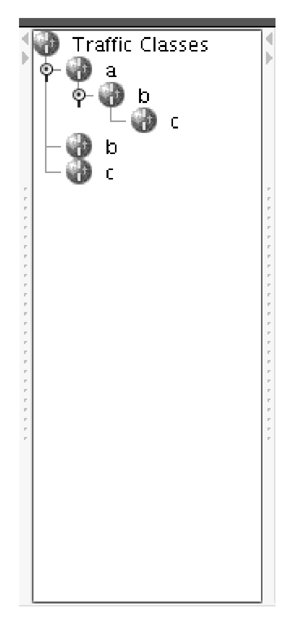


Figura 76. El árbol de jerarquía de clases

10.1.2 Políticas de Tráfico

Una política de tráfico es un objeto que se asocial a una o más clases y una o más interfaces.la configuración de clases asignadas a la política de tráfico, define la política para las interfaces asociadas. La manera en que usted asigna clases a políticas es ilimitada. Las políticas de clases pueden ser compartidas por muchas interfaces, en cuyo caso las interfaces son unificadas desde el punto de vista de la calidad de servicio. Las políticas compartidas serán discutidas con más detalle en un capítulo posterior.

10.1.3 Interfaces de Red

Este panel enlista todas las interfaces físicas del sistema. Para cada interfaz, se distinguen dos flujos: uno de entrada, el cual corresponde al tráfico entrante a la interfaz, uno de salida, que corresponde al tráfico de salida de la interfaz.

> ***Nota**: los Bridges e interfaces virtuales no estarán presentes aquí. Si usted desea configurar una política al bridge, configure la misma política de tráfico a cada interfaz física que pertenece al bridge. Las interfaces virtuales pueden solo ser distinguidas basadas en su dirección IP.*

Mantenga en mente, que usted no puede asignar más de una política por flujo de interfaz; así como la misma política para ambos flujos de la misma interfaz.

La manera en que las clases, políticas e interfaces están inter relacionados está representada en la figura 79.

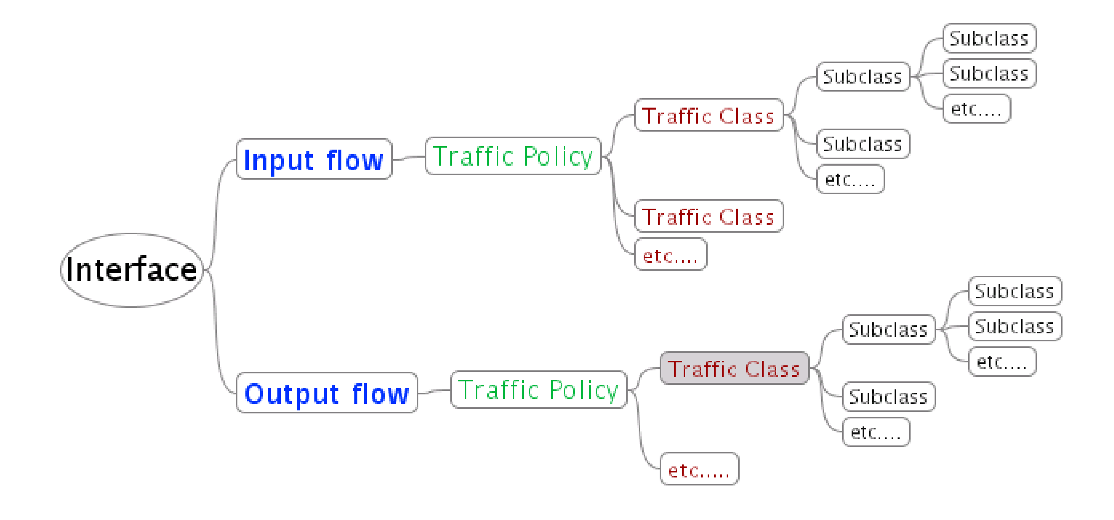


Figura 77. Clases, Políticas e Interfaces

Las asociaciones se llevan a cabo mediante arrastrar y soltar un ítem en otro.

10.2 Diferenciando el tráfico de Red

El tráfico de red puede ser categorizado por casi todo tipo de combinación de las siguientes propiedades.

Entrada/Salida Interfaz	Eth0 in, ath0 out
Origen/Destino IP	192.168.2.0/24, 172.16.1.1/32
Origen/Destino Puerto	0-1024, 520
Origen/Destino Mac	01:02:03:04:05:06
Protocolo	IP, TCP, UDP, ICMP,...
Aplicación	tráfico P2P, etc.
Negociación de la mayor parte mencionada	! 192.168.1.1/32

Estos parámetros constituyen la parte de CONCORDANCIA de una clase. El panel responsable para estas opciones está en la figura 80.

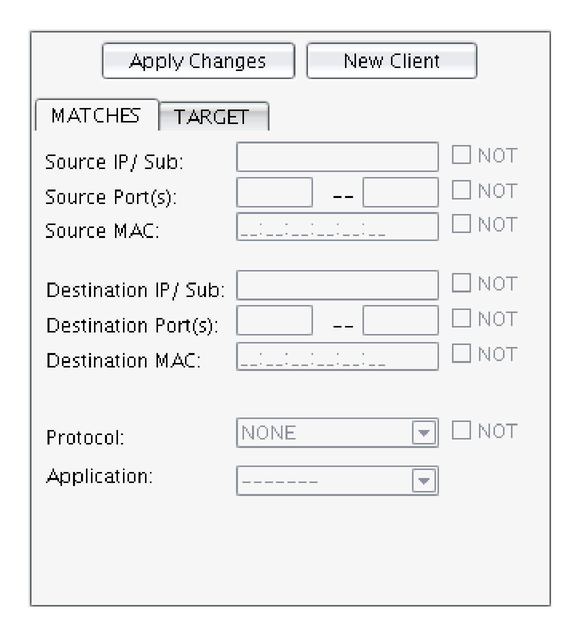


Figure 78. Network Traffic Matches

10.3 Garantías y Limitaciones

De otro lado, los recursos de red que pueden ser garantizados o limitados son:

- Taza de información comprometida
- Información sobre tasas de pico
- Committed Burst Size
- Excess Burst Size
- Prioridad

Estos parámetros constituyen el objetivo de una clase. El GUI responsable para estas opciones se muestra en la figura 81.

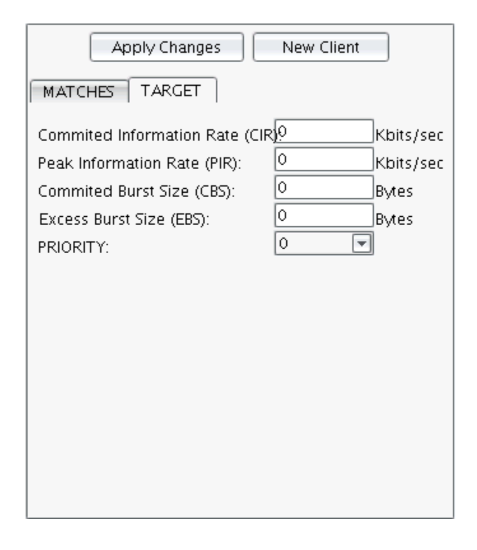


Figura 79. Parámetros de una Política

10.3.1 Taza de información comprometida (CIR)

Esta es la velocidad (expresada en kbits/s) que es garantizada y que siempre estará disponible para la respectiva clase de tráfico. Aparentemente, el CIF dedicado para una clase específica, no puede exceder el ancho de banda disponible de la red. Cuando múltiples clases que compiten existen para la misma interfaz y la misma dirección (output/input), la suma de todos ellos debería también no sobrepasar el ancho de banda disponible.

Note que, sin tener en cuenta el CIR el tráfico es siempre transmitido a la máxima velocidad soportada por la interfaz física. Literalmente, el CIR expresa la velocidad promedio a la cual el tráfico es enviado.

10.3.2 Taza de Información de Picos (PIR)

Esta es la máxima velocidad (en kbits/s) a la cual el tráfico de una clase, puede ser enviado o recibido (en promedio). Incluso si ningún otro tráfico compite por el ancho de banda, esta barrera no puede ser excedida. Este valor puede ser tan grande como la capacidad del enlace y tan pequeña como el CIR.

El ancho de banda entre CIR y PIR no está garantizado para una clase. La posibilidad para una clase de explotar este rango, depende en su prioridad como se verá más adelante.

10.3.3 Excess Burst Size (EBS)

Algunas aplicaciones están caracterizadas por cortos periodos del uso intensivo de la red y largos periodos sin ningún uso de esta. Por ejemplo, cuando se busca en Internet, el buscador web solicita una página web y luego queda inactive por un largo periodo de tiempo, hasta que otra página se solicite.

Estas aplicaciones no son bien servidas solo por el mecanismo CIR/PIR. El mecanismo EBS remedia este problema permitiendo una aplicación enviar un número de bytes continuamente por algún tiempo sin ser interrumpida. Tan pronto como los EBC bytes hayan sido enviados, la aplicación es forzada a regresar a su comportamiento normal (al promedio entre CIR y PIR).

10.3.4 Committed Burst Size (CBS)

El CBS corresponde al mínimo número de bytes que tienen que estar disponibles para que una transmisión empiece. Al momento que la transmisión empiece no es posible que sea interrumpida hasta que no haiga otro dato para enviarse. Por defecto este valor es el más pequeño posible (el tamaño de un paquete ideal) y apenas usted tendrá que configurar un valor diferente.

Para entender mejor el concepto de taza y burst, considere la siguiente analogía: cada clase (o sub clase como se verá más adelante) es como un cubo con tamaño EBS. El cubo se llena a una velocidad cuyo rango es entre CIR y PIR. De acuerdo con esta analogía, las transmisiones empiezan cuando se tira agua fuera del cubo. La mínima cantidad de agua (tráfico) que se puede tirar es CBS. Por lo tanto, cuando una clase se inactive por un momento es posible que una aplicación más adelante envíe una gran cantidad de datos hasta que el cubo se vacíe. Similarmente, para una clase que envía tráfico a un ritmo constante menor que el CIR, el cubo siempre se llenará.

10.3.5 Prioridad

El valor de prioridad dicta que clase entre aquellas de la misma capa no usará ancho de banda. Este ancho de banda viene desde aquellas clases que no están usando completamente su CIR. Este extra ancho de banda se entrega primero a la clase con la más alta prioridad y tan pronto como el PIR (o EBS) de esta clase se alcance, la distribución continua en orden de prioridad. El valor de la prioridad puede variar entre 0 (la más alta prioridad) y 7 (la prioridad más baja).

Considere el siguiente escenario: se tiene un enlace estándar inalámbrico de 11Mbps, y se quiere garantizar la mitad de este para el tráfico de salida TCP. Luego se divide el tráfico destinado TCP para el host x y que está destinado al host y. este escenario se explica en la siguiente tabla.

Las clase en la tabla denotadas como “auto”, son clases que son automáticamente (y transparentemente) creadas por el sistema para manejar tráfico no clasificado. Estas clases automáticamente generadas consiguen el resto del ancho de banda (como su CIR) el cual no está reservado para cualquier usuario. El sistema genera clases siempre con una prioridad de 7.

<table>
<tr><th colspan="4">Ancho de Banda Enlace 11Mbps</th></tr>
<tr><td colspan="3">USER CLASS</td><td>AUTO CLASS</td></tr>
<tr><td colspan="3">CIR 5,5 mbps: Outgoing TCP</td><td>CIR 5,5 mbps: Anything but TCP</td></tr>
<tr><td colspan="3">Priority 0</td><td>Priority 7</td></tr>
<tr><td>USER SUBCLASS 1</td><td>USER SUBCLASS 2</td><td>AUTO SUBCLASS</td><td rowspan="3">No subclasses available</td></tr>
<tr><td>1,8 mbps
host x</td><td>1,8 mbps
host y</td><td>Rest traffic
(1,8 mbps)</td></tr>
<tr><td>Priority 0</td><td>Priority 1</td><td>Priority 7</td></tr>
</table>

De regreso al escenario:

Vamos a asumir ahora que 7 Mbps de tráfico (fuera de 11 Mbps) califica para la clase USER. Esto significa que se tiene 7Mbps de tráfico TCP el cual tiene que ser distribuido entre las subclases. Asumamos también que 1/3 de este tráfico está destinado para el host x y otro 1/3 para el host y. aunque podría ser tentador decir que sus subclases obtendrán 1/3 de los 7Mbps, por lo tanto SUBCLASS 2 y AUTO SUBCLASS obtendrán exactamente 1.8Mbps (el CIR) y SUBCLASS 1 obtendrá 3.4Mbps. Esto es ya que SUBCLASS 1 tiene una mayor prioridad. Si no hay tráfico del todo para SUBCLASS 1, luego SUBCLASS 2 obtendrá 5.2 de los 7Mbps disponibles. Por ahora, el rol de prioridad debería estar claro.

10.4 Ejemplo: Reservación de ANCHO DE BANDA para Servidores FTP

Veamos ahora un ejemplo, para comprender mejor el mecanismo de QoS. Digamos que tenemos un NETKROM OS Hotspot, equipado con un enlace inalámbrico estándar de 11Mbps. El ancho de banda real disponible en una interfaz es aproximadamente 5.5Mbps. En el lado Ethernet hay dos servidores FTP y un grupo de otros host insignificantes. El servidor FTP sirve a los clientes hotspot. Por lo tanto, nos gustaría garantizar un poco de ancho de banda para ellos. La capa de red se ilustra en la figura 82.

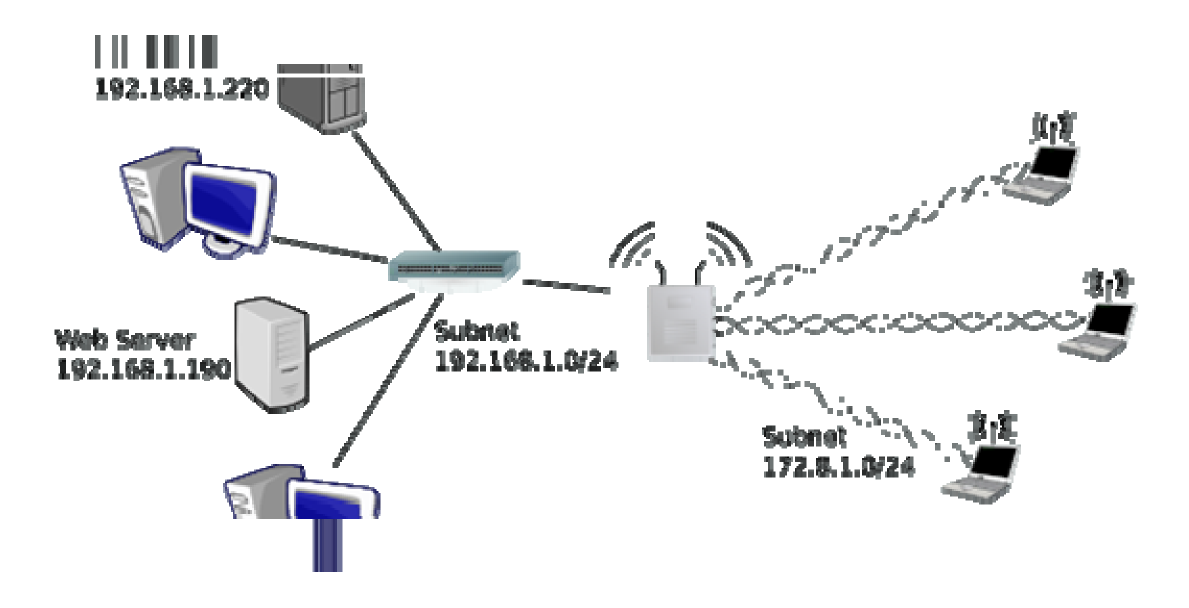


Figura 80. Hotspot con dos servidores FTP

10.4.1 Clase Individual por Política

Se empezará por definir una política de QoS para garantizar 3 Mbps para tráfico FTP. Ya que se quiere garantizar ambos el tráfico de subida y de bajada desde el servidor FTP, se creará dos clases diferentes, una para cada dirección de flujo. En cada uno de ellos se configurará un límite de PIR (3.5 MBPS) para prevenir al servidor FTP de monopolizar el ancho de banda.

Pasos a seguir:

1. Click en "Traffic Classes" y click derecho sobre este.
2. Agregar una nueva clase llamada "ftp_traffic_out", para manejar el tráfico de salida desde la interfaz ath0.
3. Click en la clase "ftp_traffic_out" y configure las concordancias y objetivos como se muestra en la figura 83.

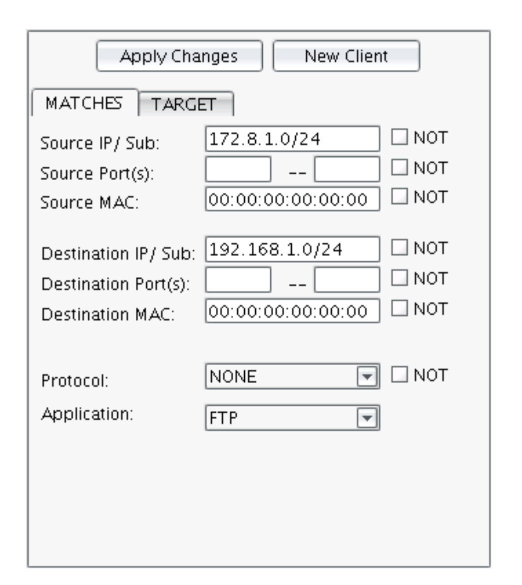


Figura 81.

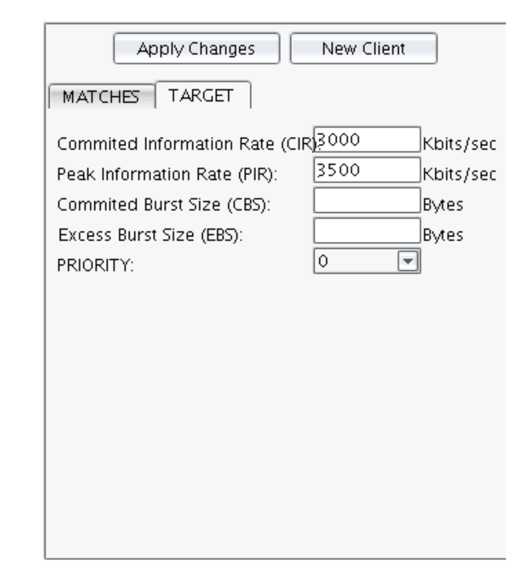


Figura 82. Configuración 'ftp_traffic_out'

4. Similarmente, se configure una clase 'ftp_traffic_in' para la dirección de flujo de entrada. (Figura 84).

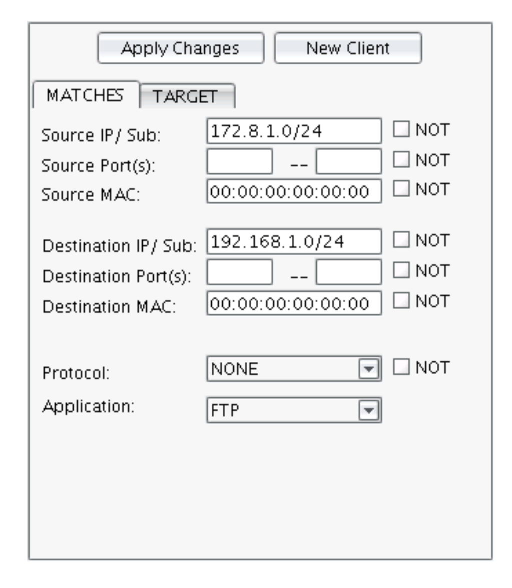


Figura 83.

Figura 84. Configuración 'ftp_traffic_in'

5 Ahora se creará dos políticas, una para cada flujo de dirección llamado 'ftp_in' y 'ftp_out'. Esto se hace haciendo click derecho en la etiqueta 'Traffic Policies'.

6. Luego se asocial cada clase a su respectiva política (figura 85). Esto se hace arrastrando y soltando las clases a las políticas y las políticas a los flujos de interfaces.

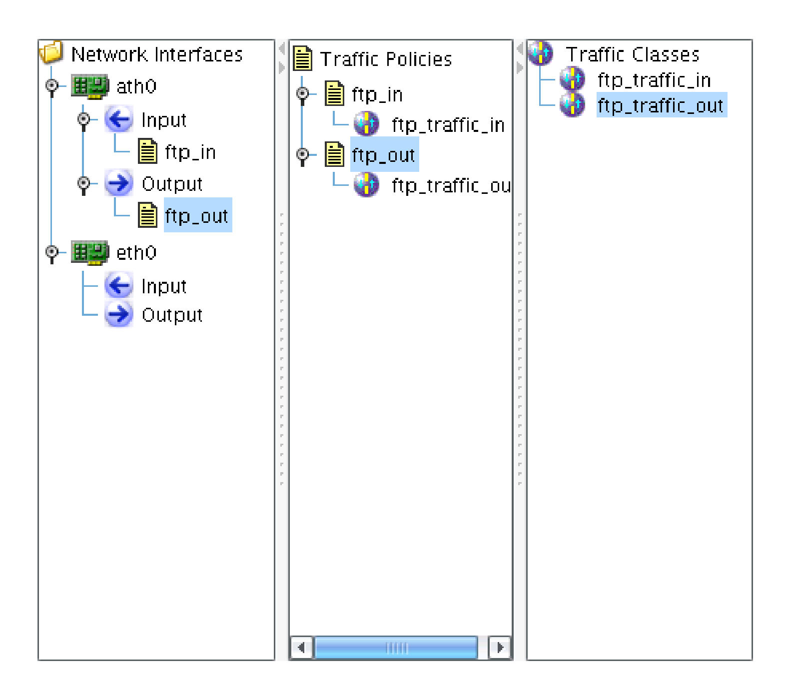


Figura 85. Clase única por Política

10.4.2 Clases Paralelas

Hasta ahora, se garantiza 3Mbps para el tráfico FTP que viene desde cualquiera de las sub redes conectadas directamente y destinada a laa otra. Sin embargo no se hace provisiones para usuarios (de cada sub red), quienes podrían configurar un servidor FTP por iniciativa propia. Estos servidores FTP pueden consumir parte de los 3Mbps, la cual está reservada para los dos servidores FTP originales. Si se quiere prevenir esto, se tendrá que ser más específico cuando se definen las clases, en particular:

1. Se renombra 'ftp_traffic_out' a 'ftp_traffic_out_ftp1' para manejar el tráfico destinado al servidor FTP 192.168.1.220. Se cambia la dirección de destino a 192.168.1.220/32. Se deja el tipo de aplicación en FTP.

2. Similarmente, se renombra 'ftp_traffic_in' a 'ftp_traffic_in_ftp1' para manejar el tráfico que se origina en el servidor FTP 192.168.1.220. Por lo tanto, se cambia la dirección de origen a 192.168.1.220/32. El tipo de aplicación FTP de objetivo se queda como está.

3. De manera similar, se crean dos nuevas clases, llamadas 'ftp_traffic_out_ftp2' y 'ftp_traffic_in_ftp2' para manejar el tráfico originado y destinado a 192.168.1.190/32 (Figura 86). También se configura la aplicación objetivo a FTP.

4. Ya que se dividió el CIR/PIR total de las clases iniciales (una para cada dirección) en dos clases, también se tiene que redefinir el CIR/PIR en cada subclase a 1500/1750. De esta manera, para cada dirección la política garantiza un CIR agregado de 3000 y un PIR agregado de 3500.

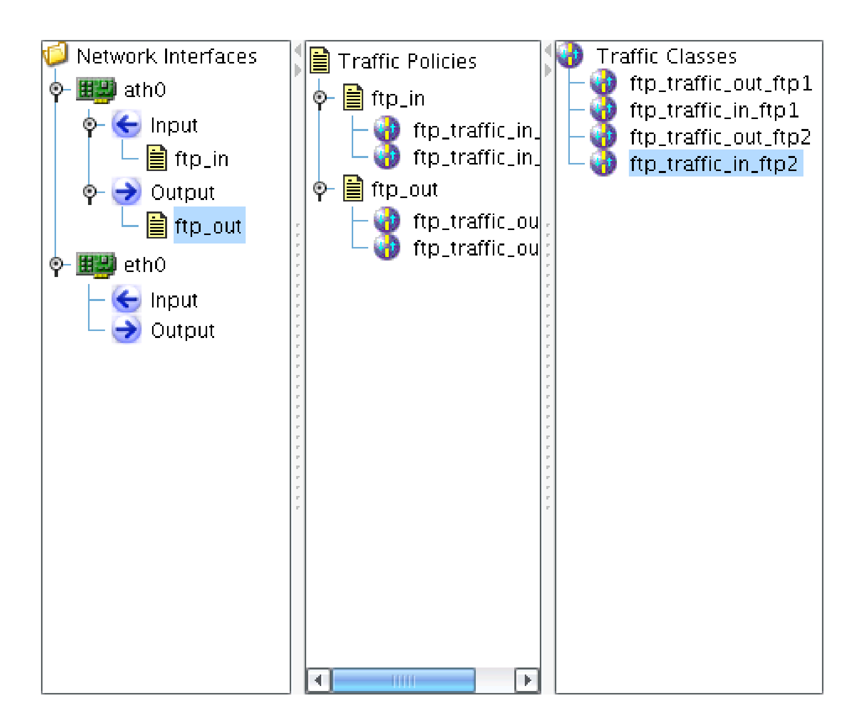
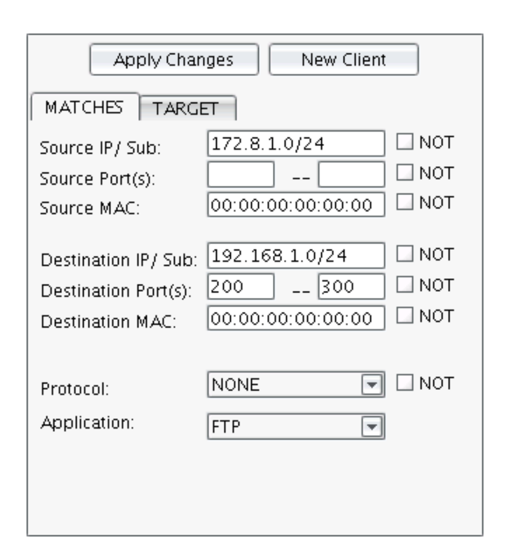


Figura 86. Clases Paralelas

Las clases 'ftp_traffic_in_ftp1' y 'ftp_traffic_in_ftp2' son consideradas como clases paralelas, como se sabe el flujo de entrada de la interfaz ath0. Esto es así ya que no forman una jerarquía y por lo tanto para cada paquete que llega, ambos son evaluados. Las clases 'ftp_traffic_out_ftp1' y 'ftp_traffic_out_ftp2' son también clases paralelas, por lo que el flujo de salida de la interfaz ath0 se refiere.

Las clases paralelas, aunque son una característica muy importante deberían ser usadas con precaución. Usted debería evitar configurar clases paralelas que se superpongan a otras. En otras palabras, debería estar claro qué clase se activará para cualquier paquete que llegue. Por ejemplo, las dos clases mostradas en la figura 87 se están superponiendo ya que son ambiguas. Una de ellas manejará el tráfico originado en la subred 172.8.1.0/24 y destinado al host 192.168.1.1/32 con número de puerto de destino 200.



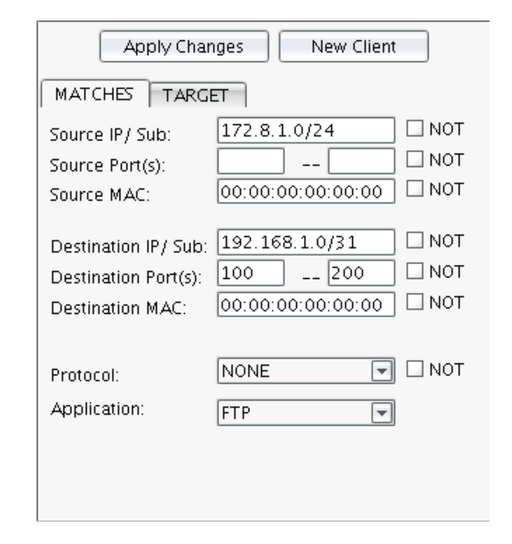
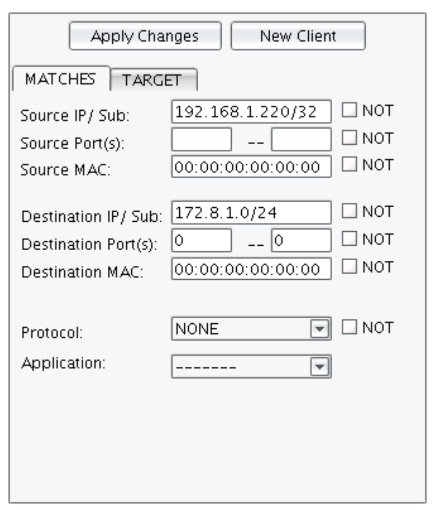


Figura 87. *Figura 88. Superposición de Clases Paralelas*

10.4.3 Clases Jerárquicas

Aunque el tráfico agregado FTP cae dentro de los límites (3000/3500), el máximo ancho de banda disponible para cada servidor FTP se restringe a 1750 Kbps, una solución intuitiva sería configurar el PIR de cada clase a 3500. Sin embargo, en ese caso, si hay harto tráfico FTP para ambos servidores, luego el tráfico FTP agregado podría exceder la restricción deseada: 3500 (ya que 3500+3500=7000). Para aliviar este problema, se tundra que crear una clase jerárquica.

1. Se configura el CIR/PIR de cada clase creada hasta ahora a 1499/3500 y se elimina el tipo de aplicación de FTP.
2. se crean dos nuevas clases, llamadas 'ftp_traffic_in' y 'ftp_traffic_out'. Se configure el CIR/PIR en cada una de ellas a 3000/3500. El origen IP/Sub de 'ftp_traffic_in' debería ser configurada a 192.168.1.0/24 y el destino IP/Sub de 'ftp_traffic_out' a 192.168.1.0/24. Esto es para permitir que otras sesiones FTP tomen lugar. Luego, en la parte de concordancias se configure el rango de puertos de 20-21 (ftp-datos, ftp-control), y el tipo de protocolo a FTP.



ftp_traffic_in_ftp1

Apply Changes
New Client
MATCHES
TARGET
Source IP/ Sub: 172.8.1.0/24 NOT
Source Port(s): -- NOT
Source MAC: 00:00:00:00:00:00 NOT
Destination IP/ Sub: 192.168.1.220/32 NOT
Destination Port(s): 0 -- 0 NOT
Destination MAC: 00:00:00:00:00:00 NOT
Protocol: NONE NOT
Application: -------

ftp_traffic_out_ftp1

Apply Changes
New Client
MATCHES
TARGET
Source IP/ Sub: 192.168.1.190/32 NOT
Source Port(s): -- NOT
Source MAC: 00:00:00:00:00:00 NOT
Destination IP/ Sub: 172.8.1.0/24 NOT
Destination Port(s): 0 -- 0 NOT
Destination MAC: 00:00:00:00:00:00 NOT
Protocol: NONE NOT
Application: -------

ftp_traffic_in_ftp2

Apply Changes
New Client
MATCHES
TARGET
Source IP/ Sub: 172.8.1.0/24 NOT
Source Port(s): -- NOT
Source MAC: 00:00:00:00:00:00 NOT
Destination IP/ Sub: 192.168.1.190/32 NOT
Destination Port(s): 0 -- 0 NOT
Destination MAC: 00:00:00:00:00:00 NOT
Protocol: NONE NOT
Application: -------

ftp_traffic_out_ftp2

Apply Changes
New Client
MATCHES
TARGET
Source IP/ Sub: 172.8.1.0/24 NOT
Source Port(s): -- NOT
Source MAC: 00:00:00:00:00:00 NOT
Destination IP/ Sub: 192.168.1.0/24 NOT
Destination Port(s): -- NOT
Destination MAC: 00:00:00:00:00:00 NOT
Protocol: NONE NOT
Application: FTP

ftp_traffic_in

Apply Changes
New Client
MATCHES
TARGET
Source IP/ Sub: 192.168.1.0/24 NOT
Source Port(s): -- NOT
Source MAC: 00:00:00:00:00:00 NOT
Destination IP/ Sub: 172.8.1.0/24 NOT
Destination Port(s): -- NOT
Destination MAC: 00:00:00:00:00:00 NOT
Protocol: NONE NOT
Application: FTP

ftp_traffic_out

3. Jale y arrastre las clases previas a estas nuevas para crear una clase jerárquica Como se muestra en la figura 89. También se altera las estructuras de las políticas para que solo las clases creadas sean asignadas a ellas.

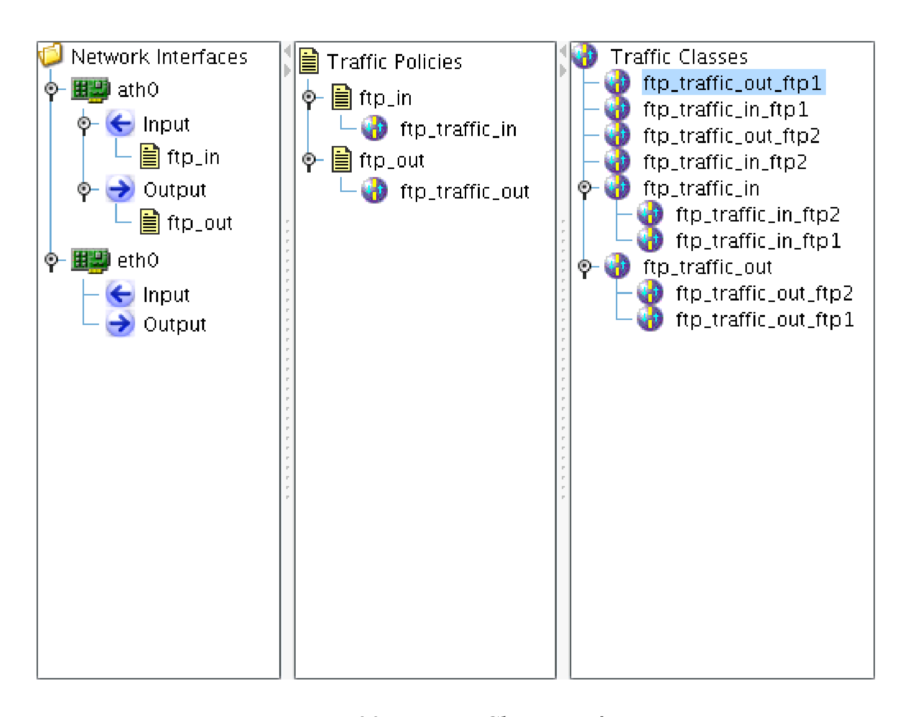


Figura 89. Clases Jerárquicas

De esta manera se limita el PIR a las clases parientes (3000/3500) y luego se distribuye en ancho de banda entre las clases hijas (1499/3500 cada una). Por lo tanto, se impone un límite superior en la cantidad de ancho de banda usado para el tráfico FTP, y al mismo tiempo se habilita ambos servidores FTP a usar el potencial completo del ancho de banda reservado.

***Note**: No se puede configurar un CIR de 1500 en cada subclase, ya que cuando se subdivide una clase en subclases, debe haber siempre ancho de banda disponible para acomodar el resto del tráfico (tráfico no cubierto por alguna de las subclases)..*

10.5 Ejemplo: Eliminación del Tráfico P2P

Actualmente, el NETKROM OS no soporta filtrado de tráfico IP basado en las propiedades de la capa 7. Por ejemplo, usted no puede configurar un firewall para bloquear tráfico entrante y/o saliente P2P. Sin embargo, usted puede eliminar virtualmente esto mediante la restricción del ancho de banda disponible a esto.

En este ejemplo se configurará dos políticas de tráfico, una para cada dirección y dos clases de tráfico que reducirán el ancho de banda disponible para el tráfico P2P tan bajo como Kbits/sec. Los usuarios P2P pronto se frustrarán y abandonarán sus aplicaciones P2P. La siguiente figura muestra la configuración de QoS que se necesita.

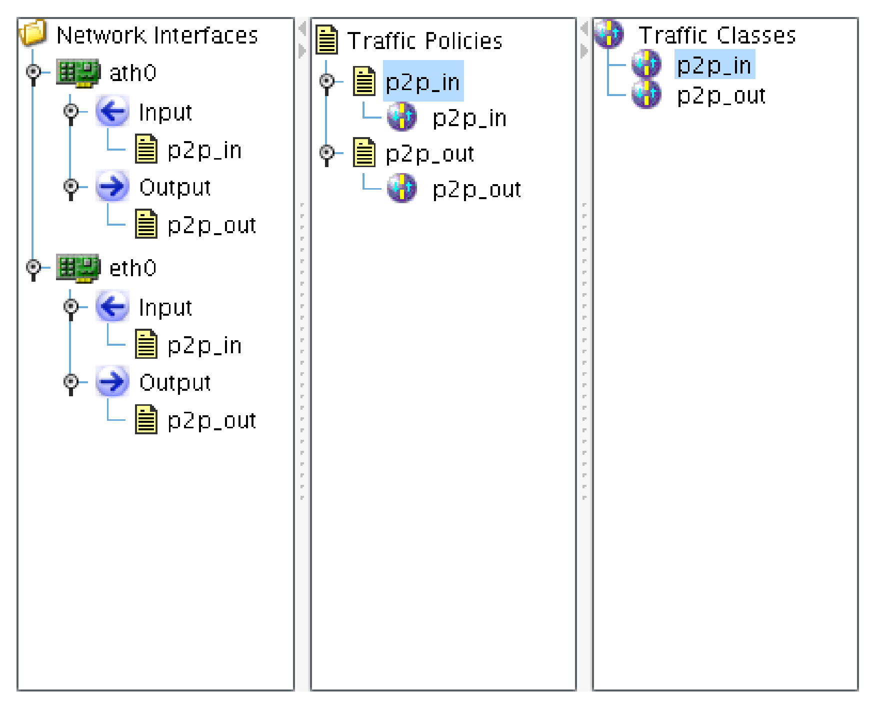
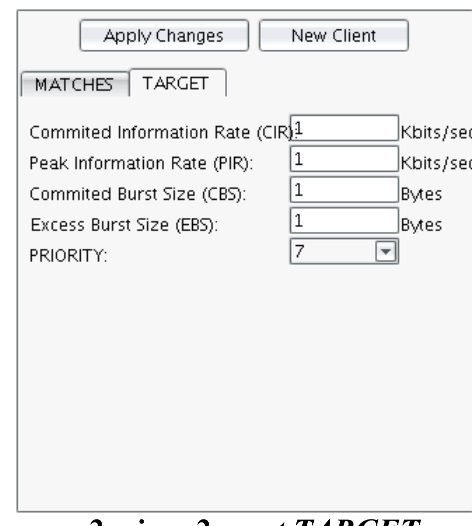


Figura 90. Clases jerárquicas para restringir el tráfico P2P en ambas interfaces

Apply Changes
New Client
MATCHES
TARGET
Source IP/ Sub: NOT
Source Port(s): -- NOT
Source MAC: 00:00:00:00:00:00 NOT
Destination IP/ Sub: NOT
Destination Port(s): -- NOT
Destination MAC: 00:00:00:00:00:00 NOT
Protocol: NONE NOT
Application: ALL PEER TO PE...

p2p_in, p2p_out MATCHES



p2p_in, p2p_out TARGET

Figura 91. Clases paralelas con superposición

10.5.1 Políticas Compartidas

En el ejemplo, las políticas de tráfico p2p_in y p2p_out son compartidas entre las interfaces eth0 y ath0. Eso las hace (ambas interfaces) ser consideradas como una única interfaz desde el punto de vista de QoS. En la práctica, esto significa que 1 Kbits/sec puede ser ocupado por tráfico P2P viniendo desde eth0 o ath0, y otro 1 Kbits/sec para tráfico P2P dejando la interfaz eth0 o ath0 (no 1 Kbits/sec cada una).

10.6 Ejemplo: Compartiendo el Ancho de Banda de un Access Point

10.6.1 Nueva Entrada QoS

NETKROM OS NNMS tiene una manera conveniente de configurar políticas de ancho de banda para clientes individuales de un access point. Esta funcionalidad solo trabaja para clientes que tienen una IP asignadas estáticamente y no vía DHCP. Si usted quiere configurar políticas de ancho de banda para clientes AP individuales que obtienen sus IP vía DHCP, usted tundra que configurar sus clases manualmente basadas en las direcciones MAC de los clientes.

Usted define una política de ancho de banda para un cliente AP haciendo click en el botón “New Client” (Figura 92).

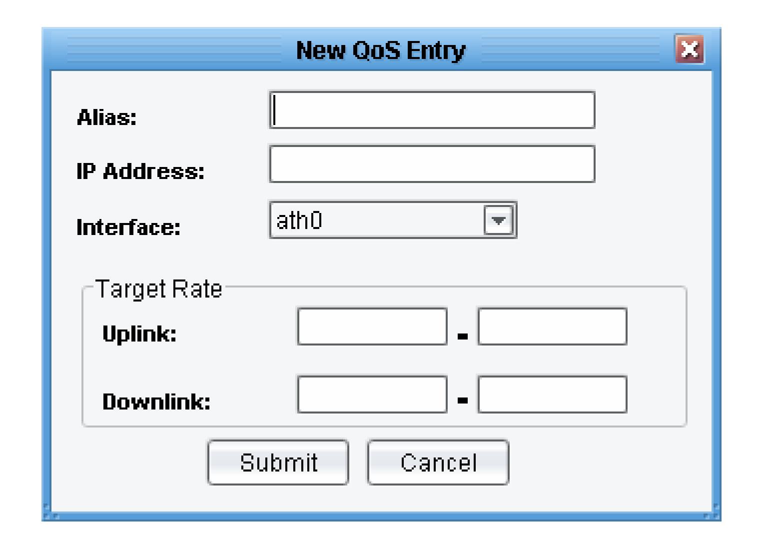


Figura 92. La ventana 'New QoS Entry'

Ahora se crearán dos políticas de ancho de banda para dos clientes AP (John y María).

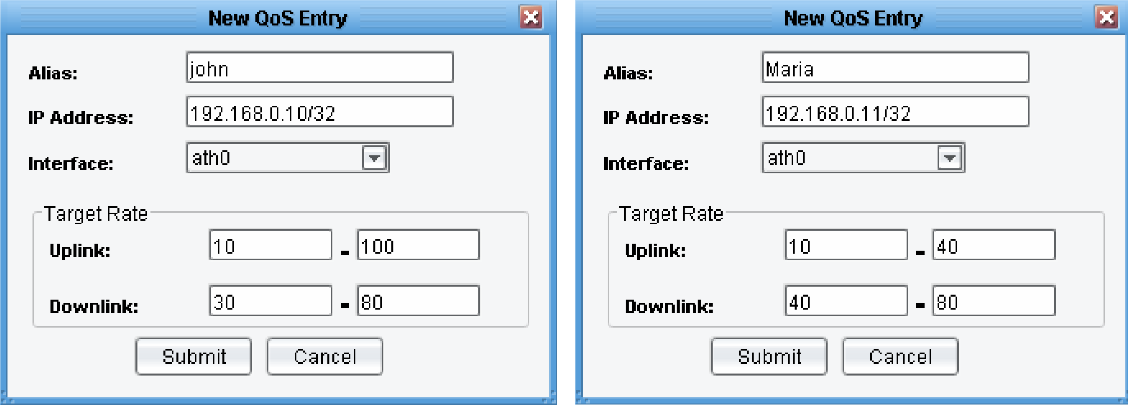


Figura 93. Configuraciones para John y María

***Nota**: Si es una dirección IP única, use una máscara de /32. Sin embargo, si usted quiere que la política cubra múltiples IPs, entonces use la máscara apropiada.*

Después de enviar ambas configuraciones, el resultado de las clases jerárquicas será este:

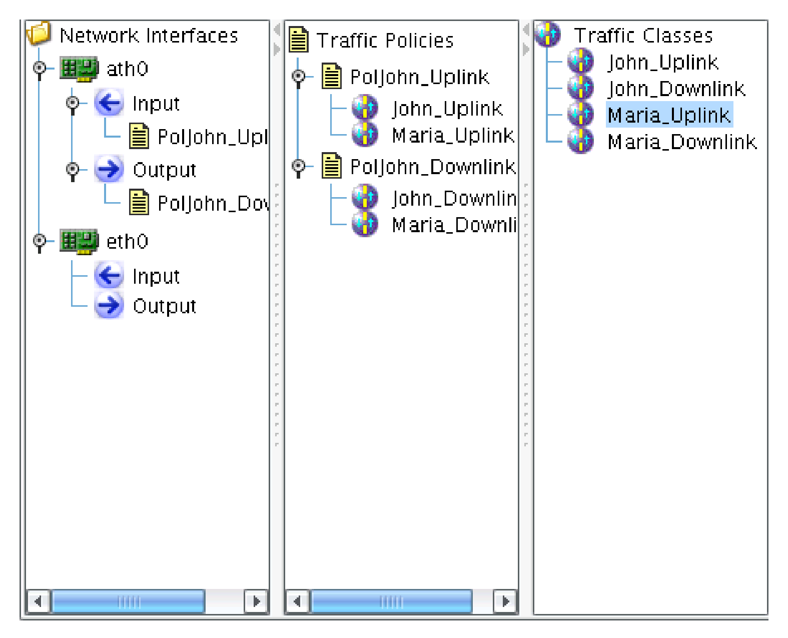


Figura 94. Resultado de la configuración de María y John

10.6.2 Estadísticas QoS

Hacienda click derecho en la política de tráfico asociada al flujo de interfaz, usted puede obtener estadísticas relacionadas a los paquetes manejados por esta política.

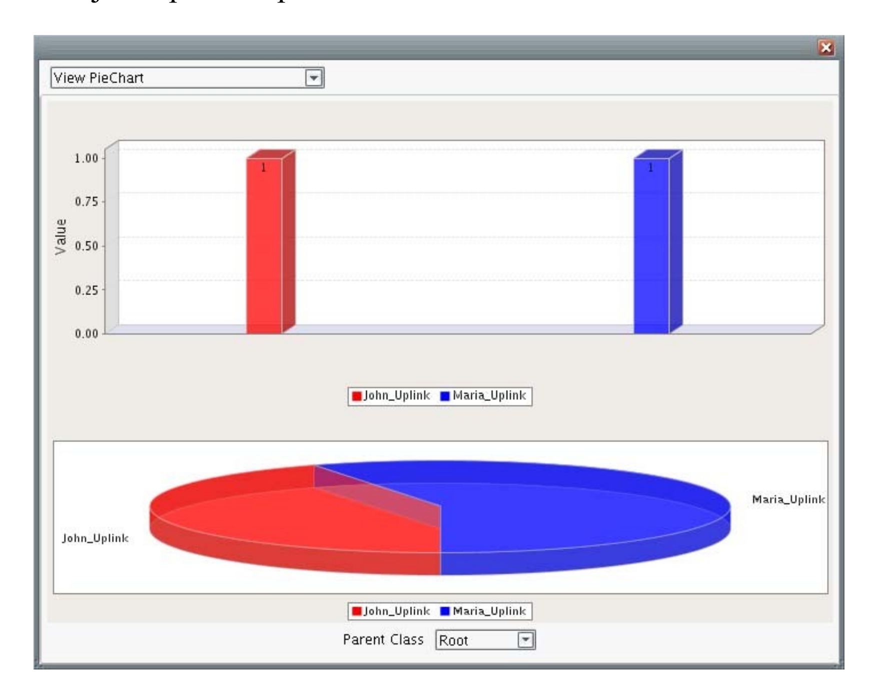
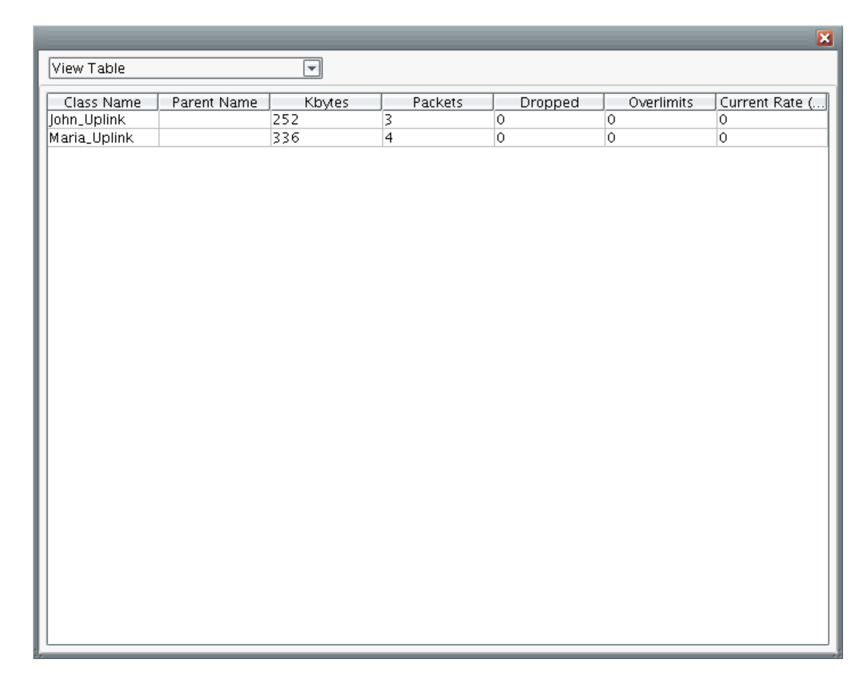


Figura 95. Estado actual

El cuadro de barras de arriba muestra la velocidad promedio actual para cada clase. El cuadro de pie corresponde al número de paquetes por la clase hasta ahora. Eligiendo la vista de la tabla usted puede obtener estadísticas más detalladas, incluyendo paquetes perdidos debido a las limitaciones de ancho de banda.



Class Name	Parent Name	Kbytes	Packets	Dropped	Overlimits	Current Rate (...
John_Uplink		252	3	0	0	0
Maria_Uplink		336	4	0	0	0

Figura 96. Estadísticas más detalladas

10.7 Diseño de Directrices y Limitaciones

10.7.1 MAC Destino/Origen

Para usar la MAC, usted tiene que configurar una interfaz bridge y asignarle la interfaz física deseada (una única interfaz está bien). Luego, usted puede usar la MAC de destino de la interfaz asignada al bridge.

También tenga en mente que en una red IP común, todos los paquetes recibidos en el gateway tienen como MAC de destino la dirección MAC del gateway. Similarmente todos los paquetes enviados por el gateway tienen como dirección MAC de origen a la dirección MAC del gateway. Por lo tanto, no tiene sentido usar estos campos en el NETKROM OS AP, el cual actúa como gateway.

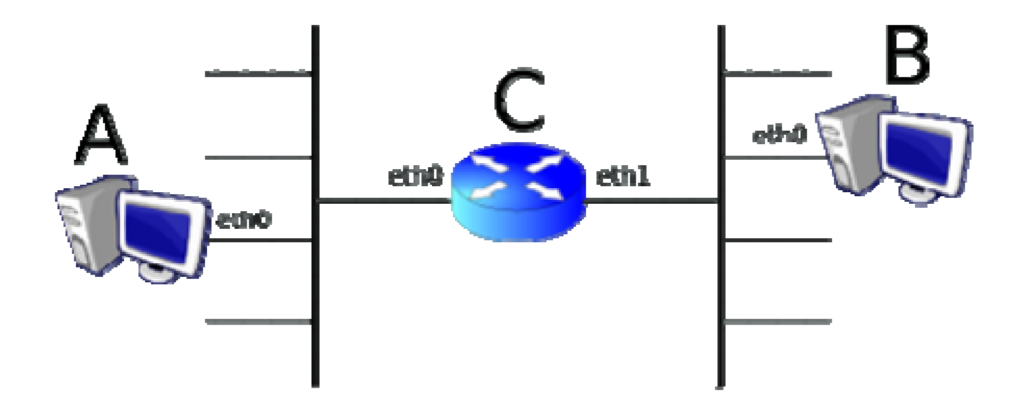


Figura 97. Un paquete enviado por A para B tiene la dirección MAC de C.Eth0 como MAC de destino, y cuando es reenviado por C, tiene como MAC de origen a C.Eth1.

Cuando A envía un paquete para B, el paquete tiene inicialmente la MAC destino como C.Eth0. Después, cuando el gateway C lo envía a B tiene como MAC de origen a C.eth1.

10.7.2 Tipo de Aplicación a Concordar

Usted puede configurar el tipo de aplicación a concordar solo en una subclase de una clase jerárquica. La razón detrás de esto es que el tipo de aplicación es muy específica y debería solo existir en subclases que residen en el último nivel de una clase jerárquica (leaf).

Además cuando el tipo de aplicación se usa, no es posible configurar el tipo de protocolo a concordar en cualquiera de las clases padres. Esto es ya que cuando usted configure un tipo de aplicación a concordar, usted implícitamente define el protocolo que corresponde al tipo de aplicación.

10.7.3 Relación de Clase de Hijo a Padre

En una clase jerárquica, la concordancia y objetivo de un hijo debería ser sub configurada en cada clase padre. Por lo tanto, usted no puede tener una clase padre para concordar un rango de puertos de destino de 1-1024, cuando uno de sus clases hijas concuerda con el rango de puertos de destino 500-2000. El rango de puertos 1025-2000 no es sub configurado en la clase padre.

10.7.4 PIR En Clases Paralelas

Actualmente, el subsistema de QoS requiere que todas las clases paralelas (o subclases) tenga un PIR definido o no. por lo tanto, no es posible configurar el PIR en una subclase ni en una clase hermana. Todas ellas deberían tener o no un PIR definido.

10.7.5 Consideraciones de Eficiencia

Siempre que sea posible, prefiera elegir el puerto o protocolo a concordar en vez de la aplicación a concordar. El tipo de aplicación a concordar es la menos recomendable.

10.8 Preguntas Frecuentes

10.8.1 Enviar, Aplicar Cambios: ¡Estoy Confundido!

El botón 'Apply Changes' es para guardar los cambios hechos en el panel más a la derecha de la interfaz QoS. Este es el panel responsable para configurar las concordancias y objetivos de las propiedades de una clase. De otro lado 'Submit' es usado para guardar la configuración total de QoS. Finalmente, no olvide guardar la configuración en el dispositivo vía la opción 'Save Configuration' en la ventana 'View Topology'.

11. HotSpot Wizard

El NETKROM OS HotSpot Access Gateway permite a los Telcos, operadores, ISPs inalámbricos, empresas, gobiernos, instituciones o escuelas implementar WLANs seguras y con autenticación. Basado en ambos RADIUS (Remote Authentication User Dial-In Service) y tecnología de redirección Web, cuando un usuario inalámbrico no autenticado intenta acceder a una página web, una página de inicio de sesión se muestra en vez de la página solicitada para que el usuario pueda escribir su nombre de usuario y contraseña y así autenticarse. Luego la información de las credenciales del usuario es enviada al servidor RADIUS para ver si el usuario tiene permisos para acceder a Internet. Este re direccionamiento web también soporta personalización de la página web, permitiendo a los operadores fácilmente designar una página web antes y/o después del inicio de sesión, sin mencionar la derivación del re direccionamiento web a los usuarios que pagan y/o aquellos que frecuentemente usan los servicios HotSpot, donde la autenticación puede ser llevada a cabo usando su dirección MAC.

Para configurar el **HotSpot Wizard**, seleccione la pestaña **HotSpot**, ubicada debajo de las pestañas **Advanced Configuration of Node, Configuration**.

11.1 Pestaña Principal del HotSpot

Cuando la pestaña HotSpot se selecciona una interfaz de usuario simple se muestra como punto inicial para el proceso de configuración del HotSpot. Desde la pestaña principal del HotSpot usted puede:

- Habilitar el HotSpot
- Ver el estado del Hotspot
- Ver la dirección MAC del administrador
- Iniciar el HotSpot Wizard
- Abrir una ventana para ver un archive que contiene información de configuración
- Abrir una ventana para ver información del usuario
- Abrir una ventana para ver las estadísticas de Radius

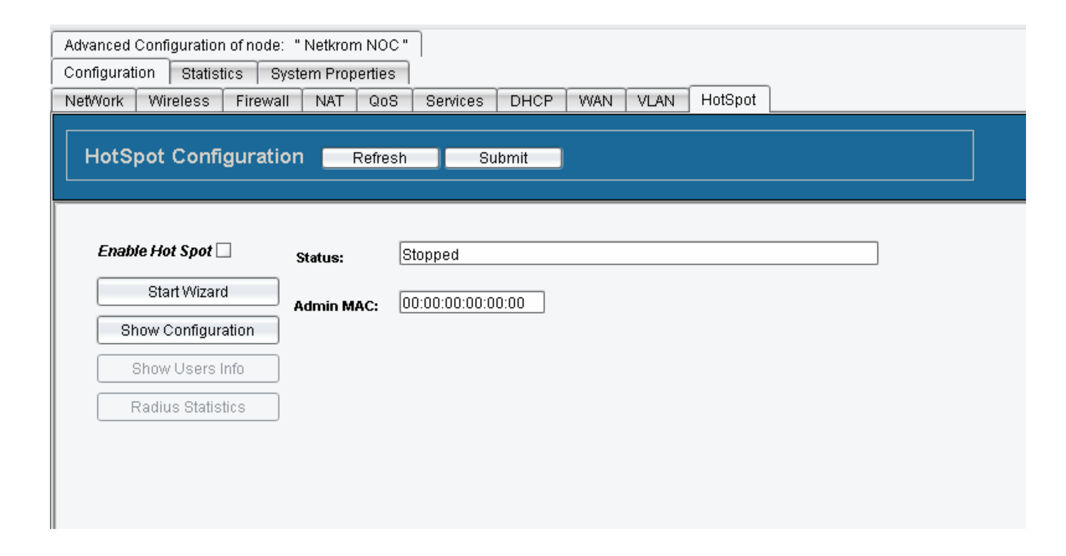


Figura 98. Pestaña principal de HotSpot

Enable HotSpot [Habilitar HotSpot]

Click en esta casilla para habilitar la funcionalidad de Hotspot.

Status [Estado]

Muestra el estado actual del HotSpot (**Stopped [Parado]**, **Running [Ejecutando]** o **Initializing [Iniciando]**). En caso de que haya un problema en la iniciación del HotSpot, un mensaje de error se muestra.

Ejemplo: DNS error El *HotSpot necesita conectarse a un servidor DNS, pero no puede encontrar uno. Esto podría ser una posible configuración incorrecta de la interfaz WAN del HotSpot o un estado temporal inalcanzable del servidor DNS (WAN no se inicia todavía o la conexión PPP no se establece todavía). El HotSpot se mantendrá reintentando de inicializar a ciertos intervalos.*

Admin MAC [MAC del Administrador]

El **Admin MAC** es la dirección MAC del administrador. Esta dirección MAC (sino ceros), siempre se considera autenticada y asignada al primer HotSpot (x.x.x.2). Configurar esto es recomendable para evitar pérdidas de conectividad con el HotSpot, si está conectado a una de sus interfaces HotSpot.

Users Info [Información de los Usuarios]

Es una lista de los usuarios que han obtenido una dirección IP, su estado de autenticación (TRUE o FALSE), y estadísticas del usuario. Para acceder a esta lista, click en el botón **Users Info**.

El botón **Users Info** está disponible cuando la configuración del HotSpot configuration está complete y el HotSpot se está ejecutando.

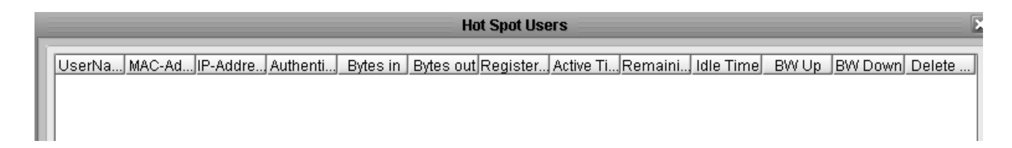


Figura 99. Ventana de información del usuario

Radius Statistics [Estadísticas de Radius]

Esta ventana le permite ver información sobre la operación del servidor Radius. Para acceder a esta ventana click en el botón **Radius Statistics**.

El botón **Radius Statistics** está disponible cuando la configuración del HotSpot está complete y el HotSpot se está ejecutando.

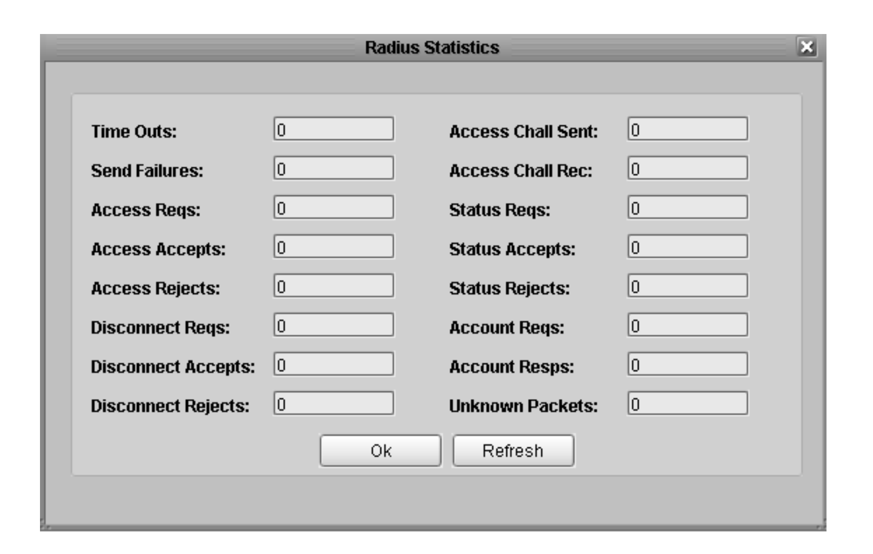


Figura 100. Ventana de estadísticas de Radius

11.2 Usando el HotSpot Wizard

Para empezar la configuración del Wizard, click en el botón **Start Wizard** en el panel de configuración. Un panel con múltiples pestañas se abre con la pestaña **WAN** en la parte superior. Para navegar entre pestañas, click en los botones **Next [Siguiente]** o **Previous [Anterior]** en la parte inferior del panel.

La siguiente sección describe la configuración de parámetros de cada pestaña.

11.2.1 WAN

WAN es la interfaz que el HotSpot debería usar para conectarse a internet.

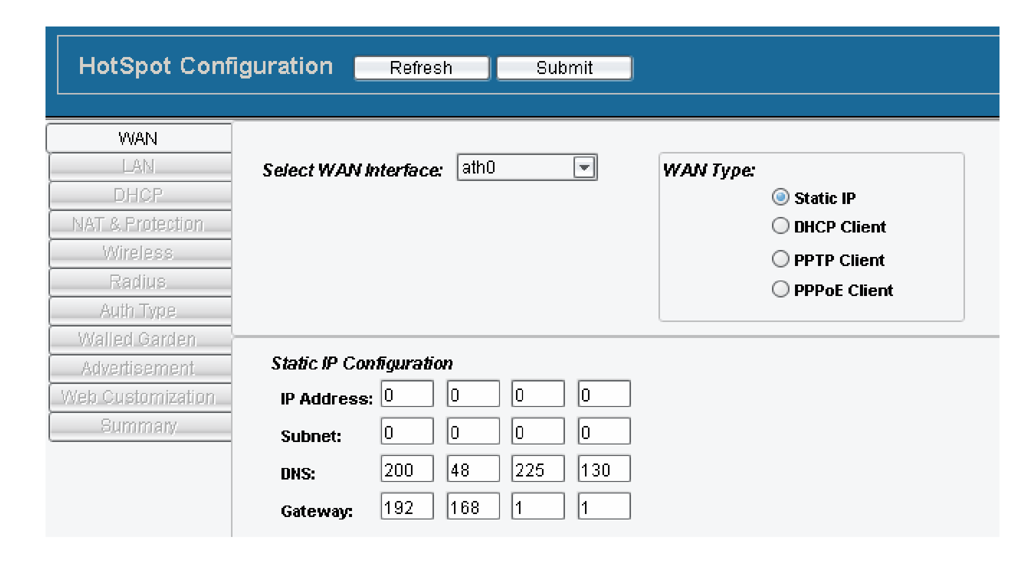


Figure 101. *Pestaña WAN del HotSpot Wizard*

Configure la pestaña WAN como sigue:

Select WAN Interface [Seleccione interfaz WAN]

Seleccione la interfaz que va a ser usada como la interfaz WAN desde la lista desplegable **Select WAN Interface**.

WAN Type [Tipo de WAN]

Seleccione uno de los siguientes tipos de WAN. Diferentes campos de configuración se habilitarán en la sección de abajo dependiendo del tipo de WAN seleccionado.

- **Static IP [IP estática o manual]**
- **DHCP Client [Cliente DHCP]**
- **PPTP Client [Cliente PPTP]**
- **PPPoE Client [Cliente PPPoE]**

Static IP [IP Estática]

A la interfaz WAN se le asignará los campos de **IP address**, **Subnet mask**, **DNS** y **Gateway**.

DHCP client [Cliente DHCP]

La interfaz WAN obtendrá los campos mencionados anteriormente a través del protocolo DHCP.

PPTP Client [Cliente PPTP]

La interfaz WAN intentará conectarse vía PPTP basado en sus parámetros de configuración.

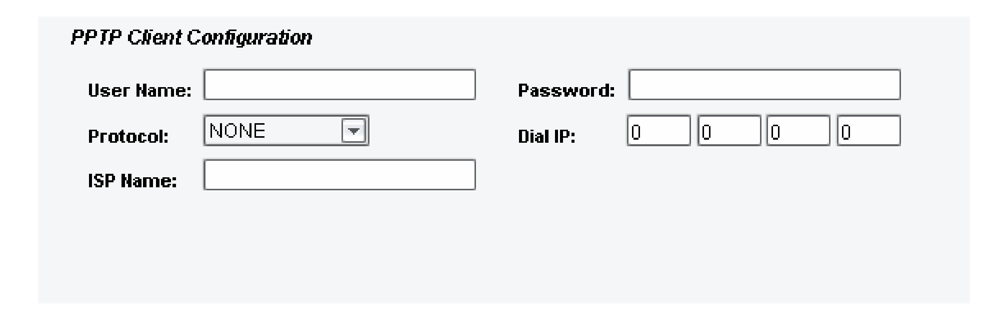


Figura 102. Configuración de un cliente HotSpot WAN PPTP

- Escriba el nombre de usuario en **User Name.**
- escriba la contraseña en **Password**.
- Seleccione **None, PAP** o **CHAP** para la autenticación.
- Escriba el nombre del ISP en **ISP Name**.
- Escriba la dirección IP dial en **Dial IP**.

PPPoE Client [Cliente PPPoE]

La interfaz WAN intentará conectarse vía PPPoE basado en sus parámetros de configuración.

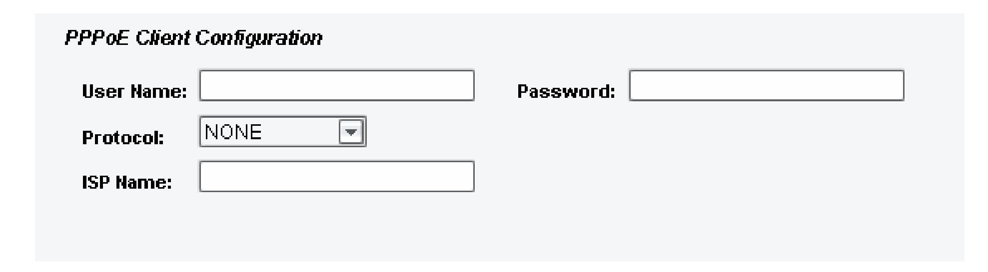


Figura 103. Configuración de un cliente HotSpot WAN PPPoE

- Escriba el nombre de usuario en **User Name.**
- escriba la contraseña en **Password**.
- Seleccione **None, PAP** o **CHAP** para la autenticación.
- Escriba el nombre del ISP en **ISP Name**.

11.2.2 LAN

Seleccione las interfaces físicas que van a ser usadas como interfaces HotSpot, luego click en el botón >>> para transferirlo al cuadro **HotSpot Interfaces**. Usted tiene la flexibilidad de seleccionar múltiples interfaces incluso Ethernet o inalámbricas. Cuando el HotSpot se inicie, estas interfaces serán puenteadas debajo de un bridge llamado br_HotSpot.



Figura 104. Pestaña LAN del HotSpot Wizard

11.2.3 DHCP

El Hotspot asignará a los usuarios HotSpot con una dirección IP en el rango de las direcciones IP dinámicas configuradas. Configure la pestaña HotSpot DHCP como sigue:

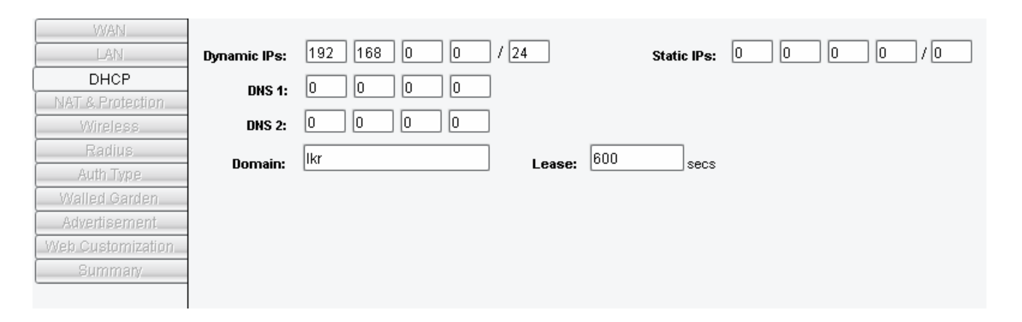


Figura 105. Pestaña HotSpot Wizard DHCP

Advertencia: Hotspot usa su servidor DHCP incorporado, el cual no se muestra en el panel de DHCP del router.

Dynamic IPs [IPs Dinámicas]

Escriba la base de direcciones IP y la máscara dentro del campo **Dynamic IPs**.

Ejemplo: Si las direcciones IP dinámicas son 192.168.1.0/24, el Hotspot asignará las direcciones IP en el rango de 192.168.1.2 a 192.168.1.254. La dirección IP 192.168.1.0 es la dirección IP de la red, la cual no puede ser asignada. La dirección IP 192.168.1.1 será asignada al mismo HotSpot (interfaz br_HotSpot). La dirección IP 192.168.1.255 es la dirección de broadcast, la cual no puede ser asignada.

DNS 1 y DNS 2

Si los valores de DNS están en 0.0.0.0, el Hotspot asignará la dirección IP del router como DNS.

Domain [Dominio]

Es el nombre del dominio signado a los usuarios HotSpot.

Lease [Arrendamiento]

Es el tiempo de arrendamiento de una dirección IP para un cliente DHCP, luego de este tiempo el cliente tendrá que renovar la dirección.

Static IP [IP Estática]

Es una opción avanzada. Usando este campo, el Hotspot nunca asignará este rango de direcciones IP, a menos que la autenticación por MAC se use y el servidor Radius fuerce una dirección IP de este rango a ser asignada.

Ejemplo: Si las direcciones IP dinámicas están configuradas como se dice arriba y las direcciones IP estáticas son 192.168.1.0/30, el Hotspot asignará las direcciones IP en el rango 192.168.1.4 a 192.168.1.254, dejando las direcciones IP 192.168.1.2 a 192.168.1.3 ser asignadas por el servidor Radius.

> ***Advertencia:*** *La subred de direcciones estáticas debería ser una subred de la subred de direcciones IP dinámicas.*

11.2.4 NAT y Protección

NAT Enable [Habilitar NAT]

Si la opción **NAT Enable** está seleccionada, las direcciones IP de los usuarios HotSpot serán traducidas a la dirección IP de la WAN. Esto se debería usar si las direcciones IPs dinámicas no son direcciones públicas IP y son privadas. Si este campo no está seleccionado, las direcciones IP de los usuarios HotSpot serán enviadas a internet sin modificación.

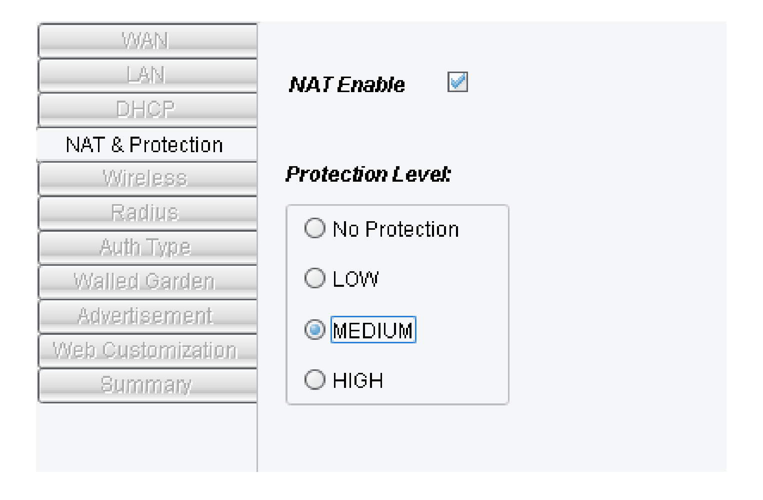


Figura 106. HotSpot Wizard NAT y la pestaña de Protección

Protection Level [Nivel de Protección]

La protección se lleva a cabo a través de las reglas del firewall. De acuerdo al nivel de protección usada se generará reglas de firewall apropiadas. (El comentario “Added_By_Hotspot” se generará automáticamente.)

Advertencia: *Todas las reglas de firewall pre configuradas serán descartadas.*

Hay cuatro niveles de protección:

No Protection [Sin Protección]

No hay protección. Todo el tráfico se acepta en ambas interfaces (WAN y HotSpot).

Low Protection [Protección Baja]

Las políticas de las cadenas de entrada del firewall serán omitidas. La siguiente configuración se aplicará al subsistema del firewall.

Tráfico Procedente de la Interfaz WAN

Tipo	Acción	Comentario
Conexión relacionada o establecida	Aceptado	Tráfico iniciado desde un router o usuarios HotSpot
Conexión SSH	Aceptado	Nueva conexión SSH
SNMP	Aceptado	Solicitud SNMP
Conexión NNMS	Aceptado	Nueva conexión NNMS
Tráfico ICMP	Limitado a 5/sec	Todo tipo de ICMP
UDP puerto 500 y Protocolos AH, ESP (IPsec)	Aceptado	Tráfico IPsec
Todo lo demás	Descartado	

Tráfico Procedente de la Interfaz HotSpot

Tipo	Acción	Comentario
Conexiones a Internet	Aceptado	Tráfico iniciado desde un router o usuarios HotSpot
Conexión SSH	Aceptado	Nueva conexión SSH
SNMP	Aceptado	Solicitud SNMP
Conexión NNMS	Aceptado	Nueva conexión NNMS
Tráfico ICMP	Limitado a 5/sec	Todo tipo de ICMP
UDP puerto 500 y Protocolos AH, ESP (IPsec)	Aceptado	Tráfico IPsec
Todo lo demás	Descartado	

Medium Protection [Protección Media]

Las políticas de las cadenas de entrada del firewall serán omitidas. La siguiente configuración se aplicará al subsistema del firewall.

Tráfico Procedente de la Interfaz WAN

Tipo	Acción	Comentario
Conexión relacionada o establecida	Aceptado	Tráfico iniciado desde un router o usuarios HotSpot
Conexión NNMS	Aceptado	Nueva conexión NNMS
Tráfico ICMP	Limitado a 5/sec	Todo tipo de ICMP
UDP puerto 500 y Protocolos AH, ESP (IPsec)	Aceptado	Tráfico IPsec
Todo lo demás	Descartado	

Tráfico Procedente de la Interfaz HotSpot

Tipo	Acción	Comentario
Conexión relacionada o establecida	Aceptado	Tráfico desde usuarios HotSpot
Conexión NNMS	Aceptado	Nueva conexión NNMS
Tráfico ICMP	Limitado a 5/sec	Todo tipo de ICMP
UDP puerto 500 y Protocolos AH, ESP (IPsec)	Aceptado	Tráfico IPsec
Todo lo demás	Descartado	

High Protection [Protección Alta]

Las políticas de las cadenas de entrada del firewall serán omitidas. La siguiente configuración se aplicará al subsistema del firewall.

***Advertencia**: La conectividad NNMS desde las interfaces WAN o Hotspot se perderá!*

Tráfico Procedente de la Interfaz WAN

Tipo	Acción	Comentario
Conexión relacionada o establecida	Aceptado	Tráfico iniciado desde un router o usuarios HotSpot
Tráfico ICMP	Limitado a 5/sec	Todo tipo de ICMP
UDP puerto 500 y Protocolos AH, ESP (IPsec)	Aceptado	Tráfico IPsec
Todo lo demás	Descartado	

Tráfico Procedente de la Interfaz HotSpot

Tipo	Acción	Comentario
Conexiones a Internet	Aceptado	Tráfico desde usuarios HotSpot
Tráfico ICMP	Limitado a 5/sec	Todo tipo de ICMP
Protocolos AH, ESP (IPsec)	Aceptado	Tráfico IPsec
Todo lo demás	Descartado	

11.2.5 Wireless

Si hay interfaces inalámbricas usadas como interfaces HotSpot, la pestaña **Wireless** se usa para configurar los parámetros inalámbricos de estas interfaces.

Por defecto, el tráfico inalámbrico a inalámbrico se descarta.

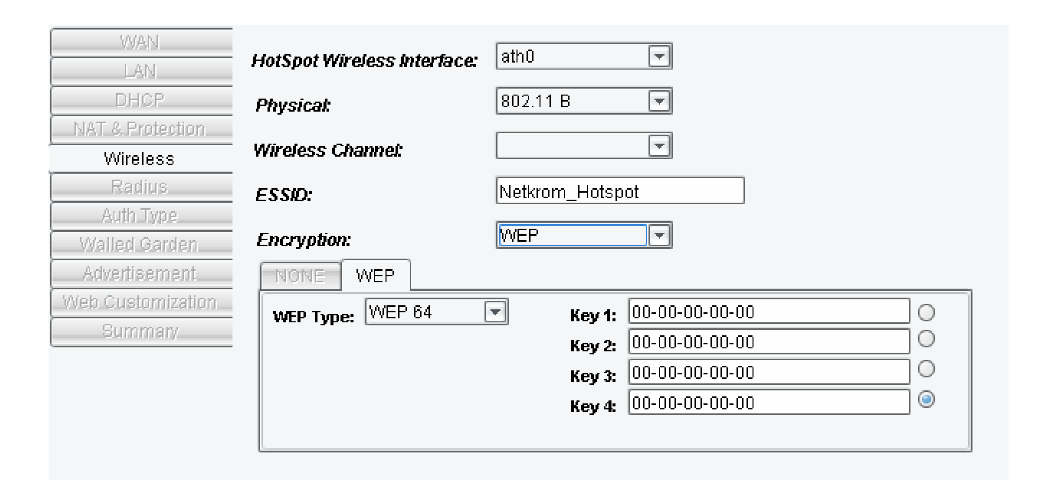


Figura 107. Pestaña Wireless de HotSpot Wizard

HotSpot Wireless Interface [Interfaz Inalámbrica del HotSpot]

Seleccione la interfaz inalámbrica para el HotSpot.

Physical [Protocolo]

Seleccione el protocolo WiFi que se usará o seleccione **Auto**.

Wireless Channel [Canal Inalámbrico]

Si se selecciona cualquier protocolo en el campo anterior excepto auto, esta lista estará disponible. Seleccione el canal inalámbrico a usar.

ESSID

Escriba el nombre de la red inalámbrica en este campo.

Encryption [Encriptación]

En esta lista desplegable seleccione entre **None** o **WEP**. Si se selecciona **WEP** campos adicionales aparecerán.

WEP Type [Tipo de WEP]

Seleccione **WEP 64** o **WEP 128** de la lista desplegable

Key 1, Key 2, Key 3 y Key 4

Escriba hasta cuatro diferentes contraseñas en estos campos y seleccione el que se usará hacienda click en el botón que está a su costado.

11.2.6 Radius

El servidor Radius que se usa para autenticar a los usuarios HotSpot.

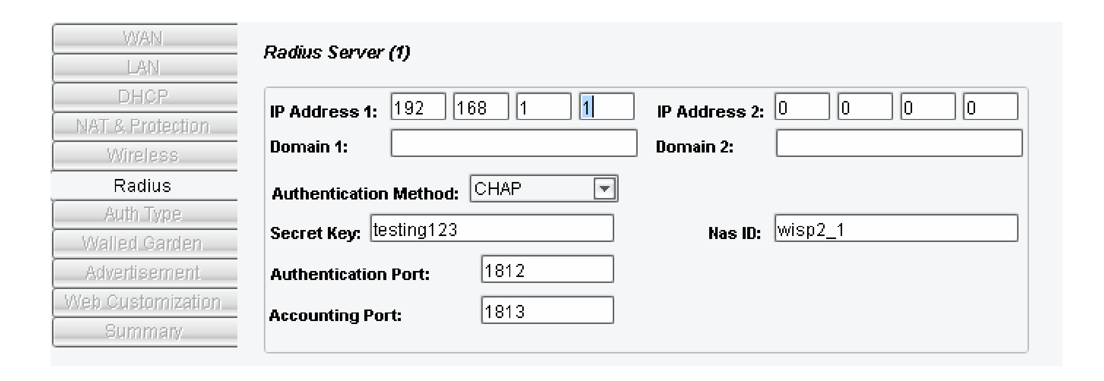


Figura 108. Pestaña Radius del HotSpot Wizard

IP Address 1 y 2 / Domain 1 y 2

Incluso la dirección IP o nombre del dominio de al menos un servidor Radius se debe configurar. El segundo servidor Radius se usa como un servidor de respaldo.

Authentication Method [Método de Autenticación]

La autorización del servidor Radius será llevado a cabo usando el método de autenticación CHAP o PAP seleccionado de la lista desplegable.

Secret Key [Clave Secreta]

Escriba la clave secreta del servidor Radius en este campo.

NAS ID

Escriba el identificador NAS del HotSpot en este cuadro.

Authentication Port [Puerto de Autenticación]

El Puerto de autenticación es el Puerto usado para enviar solicitudes de acceso al servidor Radius (1812 por defecto).

Accounting Port [Puerto de Contabilidad]

Este Puerto es usado para enviar solicitudes de conteo al servidor Radius (1813 por defecto).

11.2.7 Authentication Type [Tipo de Autenticación]

Es el método usado para autenticar a los usuarios HotSpot. Al menos uno debe de estar habilitado.

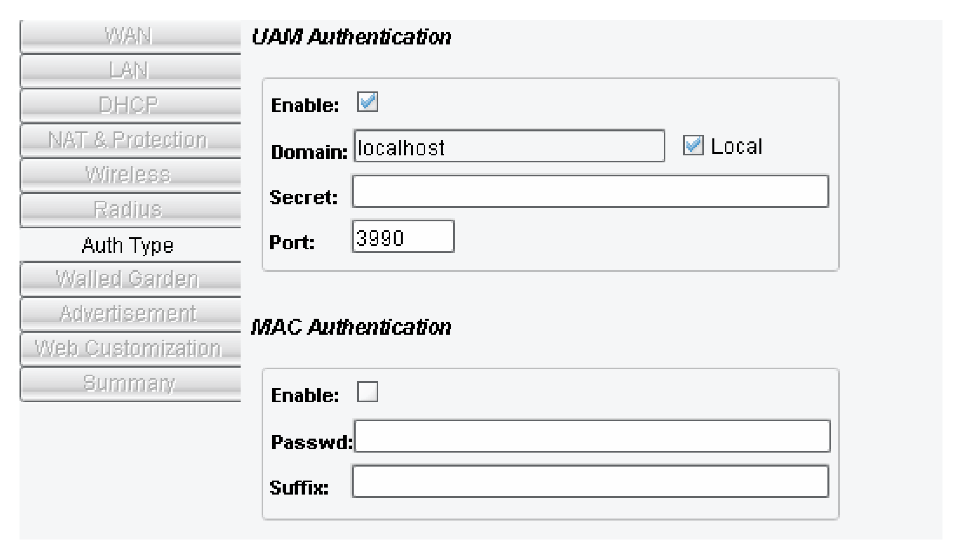


Figura 109. Pestaña Tipo de Autenticación de HotSpot Wizard

UAM Authentication [Autenticación UAM]

UAM es el tipo de autenticación de redirección web más común. Los usuarios del hotspot, después de haber obtenido una dirección IP y abierto un buscador web serán re direccionados a la página web del HotSpot para proporcionar su nombre de usuario y contraseña.

Enable [Habilitar]

Seleccione esto para habilitar la autenticación UAM**.**

Domain [Dominio]

Escriba la URL de autenticación de la página web dentro de este campo.

Secret [Secreto]

Este campo no es usado actualmente.

Port [Puerto]

El Puerto que el HotSpot usará para la redirección (Por defecto 3990).

MAC Authentication

Los usuarios Hotspot pueden ser autenticados al servidor Radius usando sus direcciones MAC (la dirección MAC para obtener una dirección IP).

El Hotspot enviará una solicitud de acceso al servidor Radius usando como nombre de usuario la dirección MAC del usuario (seguido de la cadena sufijo si está presente). También envía la contraseña configurada en el campo **Password**. Si la autenticación se completa satisfactoriamente, el usuario obtiene el Framed-IP- Address del Radius Access Response (si está presente), o la siguiente dirección IP disponible del rango de direcciones IP dinámicas. Si la autenticación falla y la autenticación UAM está habilitada, el usuario obtiene una dirección IP en el rango de las direcciones IP dinámicas y la autenticación UAM se lleva a cabo (re direccionamiento web).

Enable [Habilitar]

Seleccione esta opción para llevar a cabo la autenticación MAC**.**

Password [Contraseña]

Es la contraseña que se va a usar para autenticar a los usuarios HotSpot al servidor Radius.

Suffix [Sufijo]

Es la cadena que va junto con la dirección MAC de los usuarios HotSpot y que es usada como nombre de usuario.

> *Advertencia: si la autenticación MAC está habilitada, los usuarios del HotSpot obtendrán una dirección IP solo si el servidor Radius es alcanzable.*

11.2.8 Walled Garden

Es un conjunto de al menos 5 dominios o direcciones IP o subredes que un usuario puede accede sin haber llevado a cabo la autenticación (El usuario debe previamente obtener una dirección IP desde el HotSpot).

Escriba las URLs de estos dominios o las direcciones IP dentro de los cuadros de textos **Walled Garden URLs**.

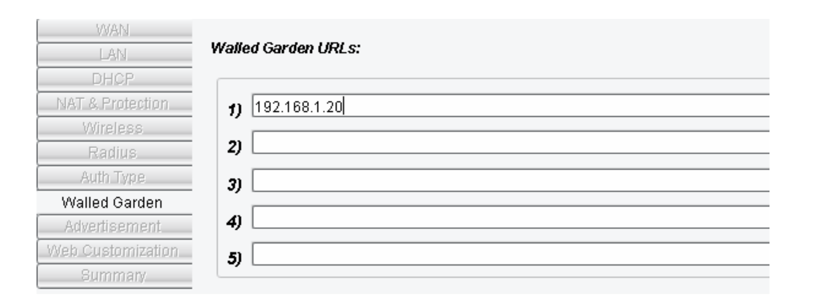


Figura 110. Pestaña Walled Garden del HotSpot Wizard

11.2.9 Advertisement [Avisos]

Es un conjunto de al menos 5 URLs a las cuales los usuarios del HotSpot serán re direccionados, después de haber sido autenticado satisfactoriamente usando UAM.

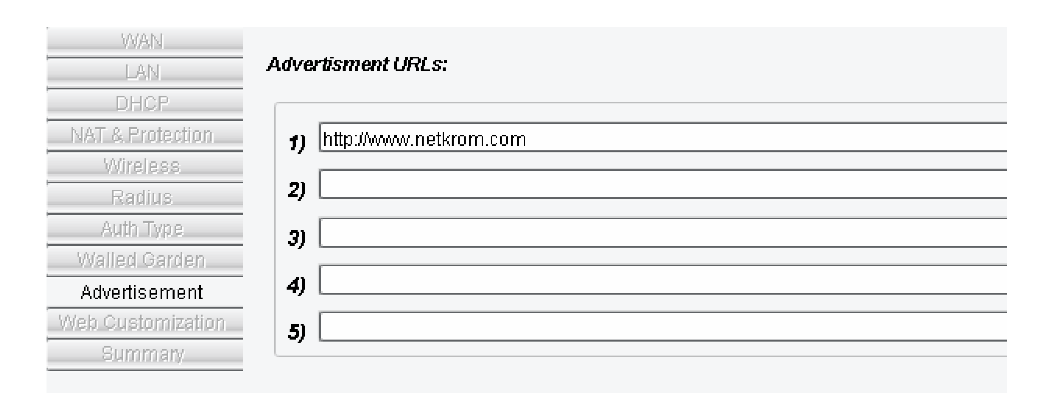


Figura 111. Pestaña de Avisos del HotSpot Wizard

11.2.10 Web Customization [Personalización Web]

Desde esta pestaña, la página web de inicio de sesión a la cual los usuarios de HotSpot son re direccionados puede ser personalizada de acuerdo a las necesidades del administrador.

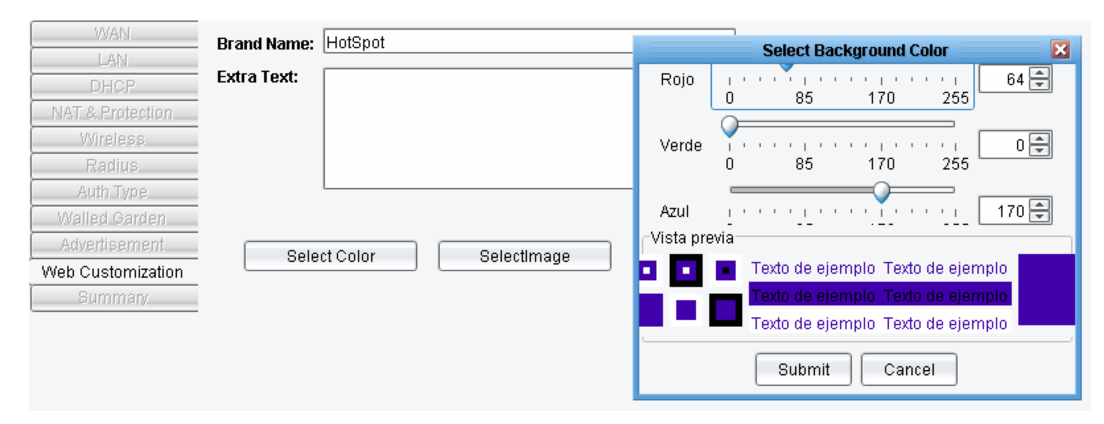


Figura 112. Pestaña de Personalización Web del HotSpot Wizard

Los siguientes campos un administrador los puede llenar con información de acuerdo a sus necesidades.

Brand Name [Nombre de Marca]

Escriba el nombre de la compañía que suministra el acceso HotSpot. Por ejemplo.
Hotspot Netkrom

Extra Text [Texto Extra]

Escriba texto adicional para propósitos promocionales. Por ejemplo, HotSpot usando el MBROMB4.

Select Color [Seleccionar Color]

Click para accede a una ventana. Seleccione el fondo de la página Web.

Select Image [Seleccionar Imagen]

Click para acceder a una ventana e importar archivos imagen de tipo .jpg, .bmp o .jpeg que se superpondrán en la página web.

11.2.11 Summary [Resumen]

Todos los datos de la configuración se muestran en esta pestaña.

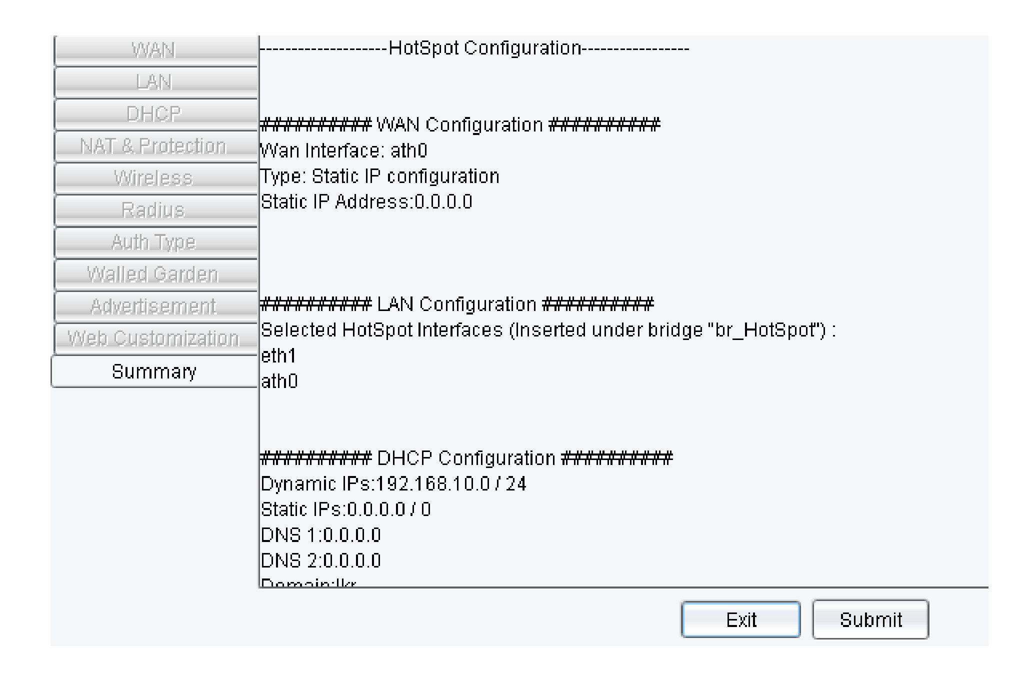


Figura 113. Pestaña Resumen del HotSpot Wizard

Submit [Enviar]

Para aplicar la configuración al MBROMB V4, click en **Submit** en la parte inferior derecha de la ventana.

Exit [Salir]

Click en **Exit** para retornar a la pestaña principal del HotSpot.

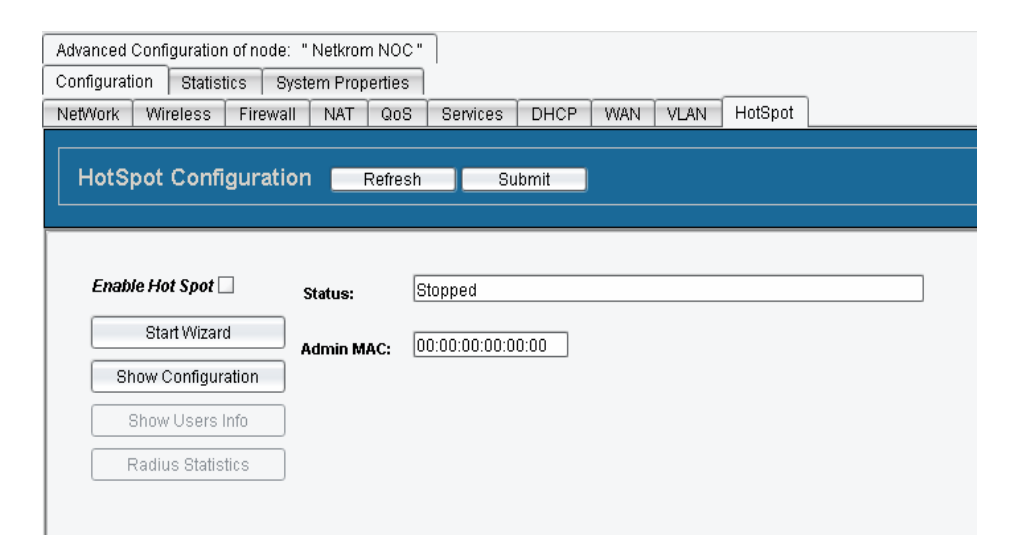


Figura 114. Pestaña Principal del HotSpot

11.2.12 Enabling the HotSpot [Habilitando el HotSpot]

En la pestaña principal del HotSpot, click en **Submit.**

Si el Hotspot ya se está ejecutando, intentará establecer la nueva configuración y empezar de nuevo. Si un error ocurre, la configuración previa se restaurará.

Si el Hotspot no se está ejecutando, la configuración se aplica pero el Hotspot permanecerá detenido.

Para hacer que el MBROMB actúe como un HotSpot, seleccione la opción **Enable HotSpot** y click en **Submit** nuevamente.

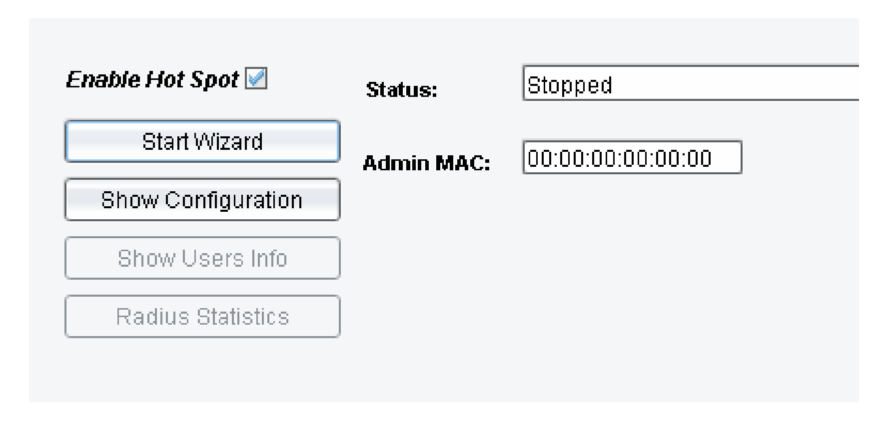


Figura 115. Iniciando el HotSpot

Para actualizar el estado del HotSpot, click en **Refresh**. Si el campo **Status** muestra **Initializing**, inténtelo unos minutes después. Si **Status** muestra **Running** quiere decir que la inicialización se ha completado.

Cuando el HotSpot se está ejecutando **Show Users Info** y **Radius Statistics** estarán disponibles.

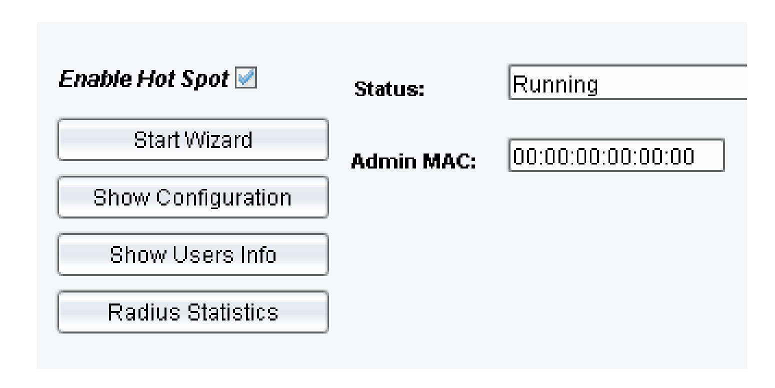


Figura 116. HotSpot Ejecutándose

11.3 Ejemplo de Configuración Radius

Lo siguiente es un ejemplo del paquete Linux free radius:

Asuma:

- La subred de IPs dinámicas es 192.168.1.0/24
- La subred de IPs estáticas es 192.168.1.0/30.
- La contraseña Radius configurada para la autenticación MAC es "password".

11.3.1 MAC Authentication

Para autenticar a un usuario usando la autenticación MAC con la MAC siguiente 000102030405, configure el servidor radius como sigue:

- 00-01-02-03-04-05* Auth-Type = Local, User-Password = "password"
- Class = 0702345678,
- Session-Timeout = 7200,
- Idle-Timeout = 600,
- Acct-Interim-Interval = 60,
- Paned-IP-Address = 192.168.1.3,
- WISPr-Bandwidth-Max-Up = 256000,
- WISPr-Bandwidth-Max-Down = 512000

***NOTA:** EL FORMATO HA SIDO CAMBIADO DESDE LA VERSIÓN 1.1.0 (XX-XX-XX-XX-XX-XX EN VEZ DE XXXXXXXXXXXX). LETRAS MAYÚSCULAS DEBEN SER USADAS (0A-0B-0C-0D-0E-0F).*

Tras la autenticación satisfactoria,

- El usuario será autenticado por 7200 segundos (2 horas), obtendrá la dirección IP 192.168.1.3, su ancho de banda de subida será 256 Kbps y su ancho de banda de bajada será 512 Kbps
- El HotSpot enviará solicitudes de cuenta al servidor Radius cada 60 segundos.

11.3.2 Autenticación UAM

Para autenticar a un usuario usando la autenticación UAM con nombre de usuario "user1" y contraseña "his_password", configure el servidor Radius como sigue:

- user1 Auth-Type = Local, User-Password = "his_password"
- Class = 0702345678,
- Session-Timeout = 7200,
- Idle-Timeout = 600,
- Acct-Interim-Interval = 60,
- WISPr-Bandwidth-Max-Up = 256000,
- WISPr-Bandwidth-Max-Down = 512000

Tras la autenticación exitosa,

- El usuario será autenticado por 7200 segundos (2 horas), con un ancho de banda de subida de 256 kbps y con un ancho de banda de bajada de 512 kbps.
- El HotSpot enviará solicitudes de cuenta al servidor Radius cada 60 segundos.

11.4 Ejemplo de Configuración HotSpot

Asuma que el sistema de los usuarios está equipado con dos interfaces Ethernet y una interfaz inalámbrica.

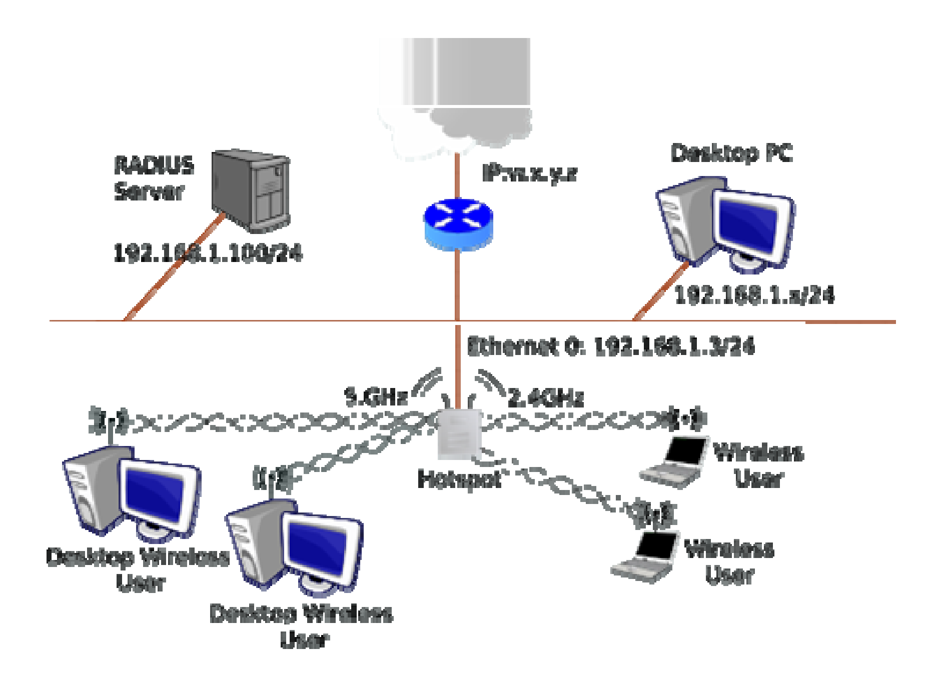


Figura 117. Ejemplo de Topología de Red

Los usuarios se conectan a internet vía un router con IP pública w.x.y.z. su red privada es 192.168.1.0/24. El router traduce las IPs privadas a su dirección IP pública.

El administrador debe autorizar a los usuarios conectados en ambas interfaces del HotSpot tanto en la interfaz Ethernet eth1 y la interfaz inalámbrica ath0. Esto se logra mediante la configuración del NETKROM como un HotSpot y autenticar a los usuarios conectados a esas interfaces. (Interfaces HotSpot).

La autenticación se asume que se llevará a cabo por el servidor Radius local (IP 192.168.1.00).

La interfaz WAN del HotSpot en este caso es eth0, que es la que está conectada al router (e Internet).

Los usuarios del Hotspot les serán asignadas las IPs de la red 192.168.0.0/24

Para resumir, el HotSpot debería estar configurado como sigue:

- Interface WAN: eth0, con IP estática IP 192.168.1.3/24
- Interfaz LAN: ath0
- Gateway: 192.168.1.1 (IP privada del router)
- DNS: por decir 65.173.1.1 (obtenido desde su conexión de internet)
- Servidor Radius: 192.168.1.100 (el radius secret es “radius_secret”)
- IPs dinámicas asignadas a los usuarios: 192.168.0.0/24

Al aplicar este ejemplo, la topología de la red cambiará a:

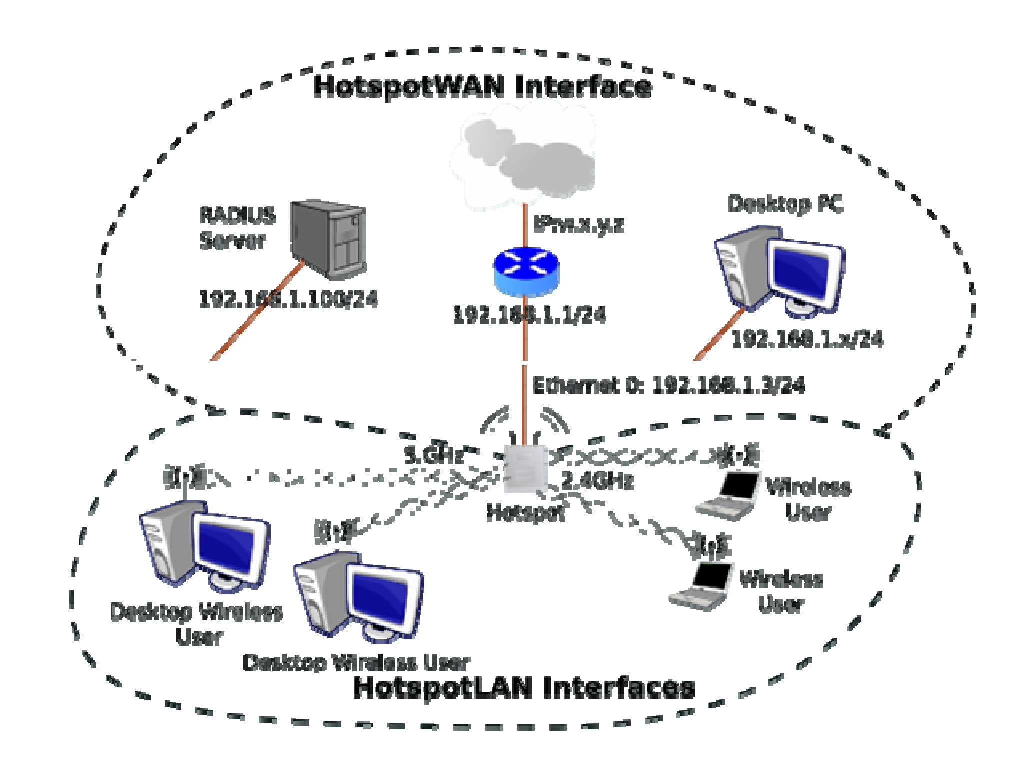


Figura 118.

En LAN (WAN para el HotSpot) no se requiere la autenticación.

En la LAN pública de los usuarios (LAN para el HotSpot) se requiere autenticación.

Procedimiento de Configuración del HotSpot

Seleccione **Advanced Node Configuration** desde **Node Shortcut Menu** en el NETKROM NMS.

Click en la pestaña **HotSpot** para empezar la configuración del HotSpot. La pestaña **HotSpot** aparece.

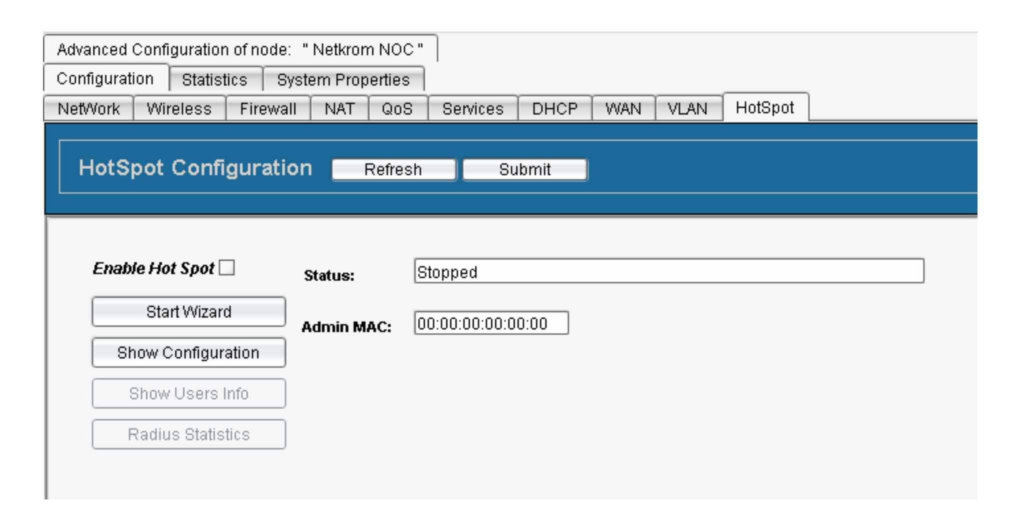


Figura 119. Ejemplo- Panel Principal del HotSpot

Click en **Start Wizard**. El panel **HotSpot Configuration** aparece conteniendo varias pestañas. La pestaña **WAN** es la primera.

1. En la lista **Select WAN Interface**, seleccione: **eth0** como la interfaz WAN
2. En **IP Address** escriba: **192.168.1.3**
3. En **Subnet** escriba: **255.255.255.0**
4. En **DNS** escriba: **65.173.1.1**
5. En **Gateway** escriba: **192.168.1.1**

Click en **Next**. La pestaña **LAN** aparecerá.

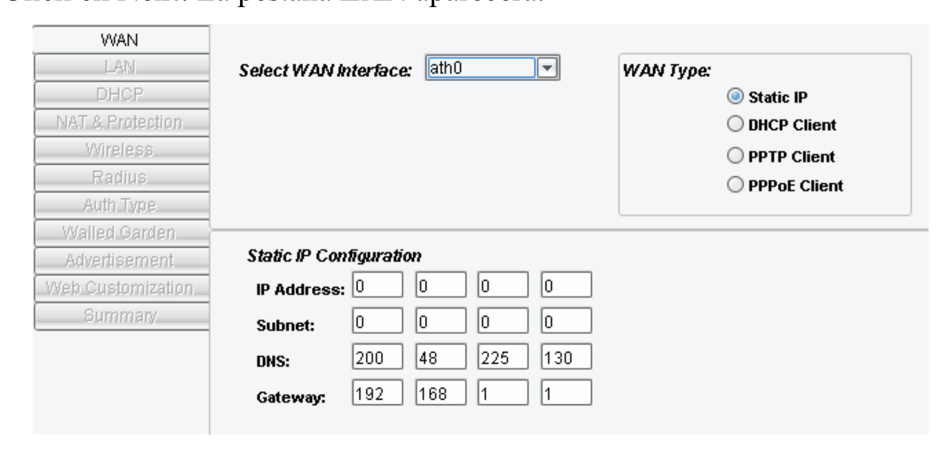


Figura 120. Pestaña WAN del Ejemplo de Configuración

La pestaña **LAN** contiene dos listas: **Physical Interfaces** y **HotSpot Interfaces**

En la lista Physical Interface, seleccione **eth1 y ath0** y cópielos a la lista

HotSpot Interface hacienda click en el botón 

Click en **Next**. La pestaña **DHCP** aparece.



Figura 121. Configuración LAN del Ejemplo

Configure los parámetros del servidor **DHCP** (las direcciones IP a ser asignadas a los usuarios HotSpot) como sigue:

1. En **Dynamic IPs** escriba: 192.168.0.0 / 24 (24 es 255.255.255.0)
2. En DNS **1 escriba**: 0.0.0.0 (esto le indicará que use el DNS de la interfaz WAN)
3. En **Domain** escriba: **domain_of_your_choice**
4. En **Lease** escriba 600, que es el tiempo de arrendamiento del

DHCP (en segundos) Click en **Next**. La pestaña **NAT & Protection** aparece.

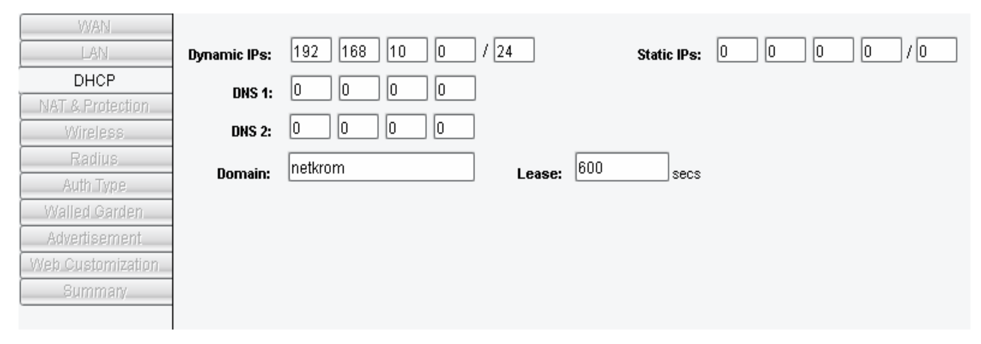


Figura 122. Configuración DHCP del Ejemplo

Configure **NAT & Protection** como sigue:

1. Seleccione **NAT Enable**. Debido a las direcciones IP dinámicas privadas del HotSpot, el Hotspot debería traducir las direcciones IP de los usuarios a la dirección IP WAN (eth0).
2. En **Protection Level**, seleccione: **Medium**.

Click en **Next**. La pestaña **Wireless** aparecerá.

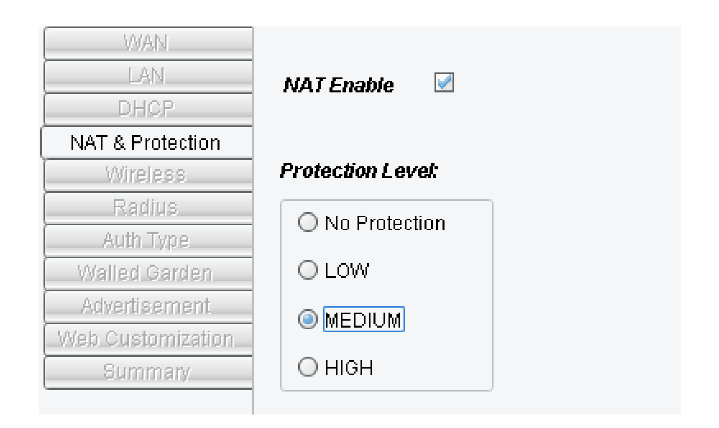


Figura 123. Configuración del NAT y del Nivel de Protección

Configure **Wireless** como sigue:

1. En la lista **Physical**, seleccione: **802.11B**
2. En la lista **Wireless Channel**, seleccione un canal
3. En **ESSID**, escriba: **My_HotSpot**
4. En **Encryption**, seleccione: **NONE**

Click en **Next**. La pestaña **Radius** aparecerá.

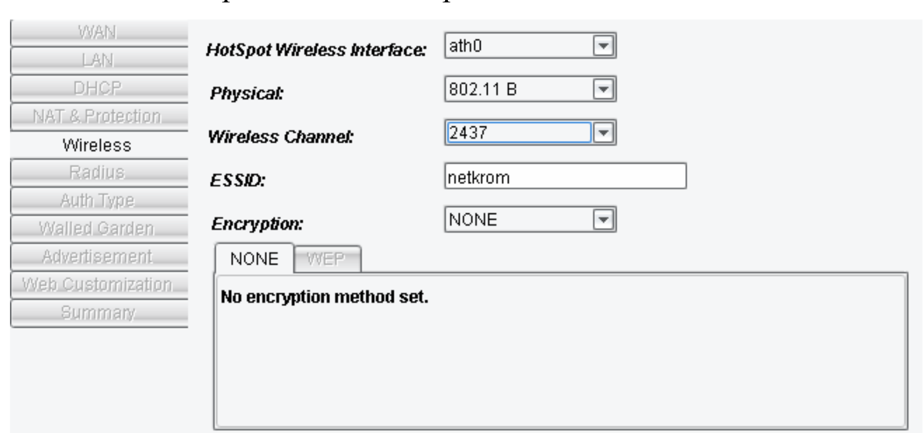


Figura 124. Configuración Wireless del Ejemplo

Configure **Radius** como sigue:

1. En **IP Address 1** escriba: 192.168.1.100
2. En **IP Address 2** escriba: 0.0.0.0 (ningún servidor de respaldo)
3. En **Authentication Method**, seleccione: CHAP
4. En **Secret Key** escriba: radius_secret
5. En **Authentication Port** escriba: 1812
6. En **Accounting Port** escriba: 1813
7. En **Nas ID** escriba: some_nas (si el servidor Radius lo necesita)

Click en **Next**. La pestaña Auth Type aparecerá.

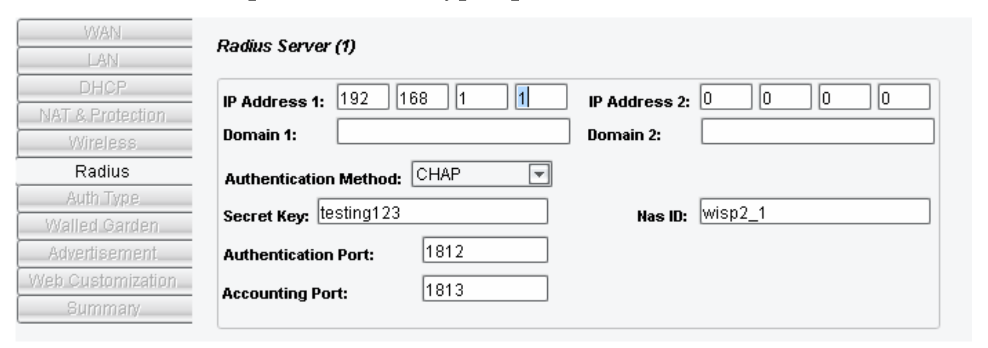


Figura 125. Configuración Radius del Ejemplo

Configure **Authentication Type** como sigue:

En UAM **Authentication**, seleccione **Enable.**

Click en **Next**. La pestaña **Walled Garden** aparece.

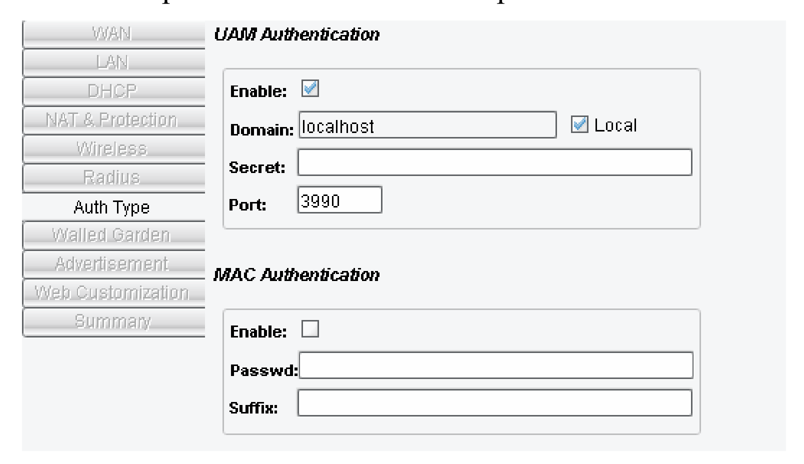


Figura 126. Tipo de Autenticación

En la pestaña **Walled Garden** usted puede configurar los dominios que un usuario puede accede sin ser autenticado. Configure el **Walled Garden** como sigue:

En **Walled Garden URLs** escriba 192.168.1.20 en el campo 1. (Para este ejemplo, esta dirección se asume que opera un servidor web público). Un usuario conectado a la interfaz LAN del HotSpot puede acceder a esa dirección IP sin autenticación.

Click en **Next**. La pestaña **Advertisement** aparece.

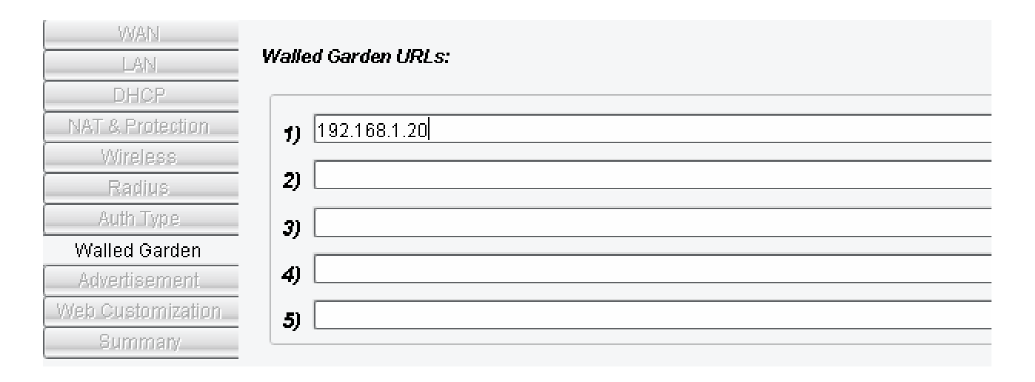


Figura 127. Configuración del Walled Garden del Ejemplo

En la pestaña **Advertisement** usted puede configurar los dominios que un usuario será direccionado después de ser autenticado. Configure **Advertisement** como sigue:

En **Advertisement URLs**, escriba la URL de cualquier página

web. Click en **Next**. La pestaña **Web Customization** aparecerá.

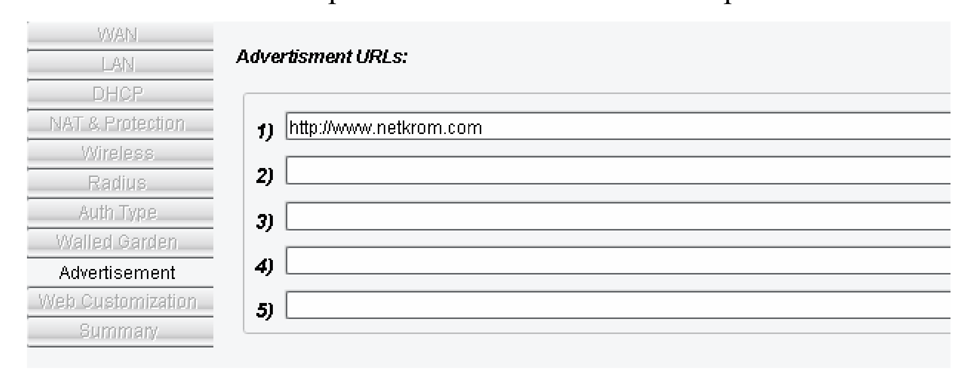


Figura 128. Configuración de Advertisement del Ejemplo

En **Web Customization** usted puede personalizar la página web de redirección. Configure **Web Customization** como sigue:

1. En **Select Background Color** establezca el color que desea
2. En **Brand Name** y **Extra Text** escriba un mensaje.
3. Click en **Select Image** y cargue una imagen para la página web.

Click en **Next**. La pestaña **Summary** aparece.

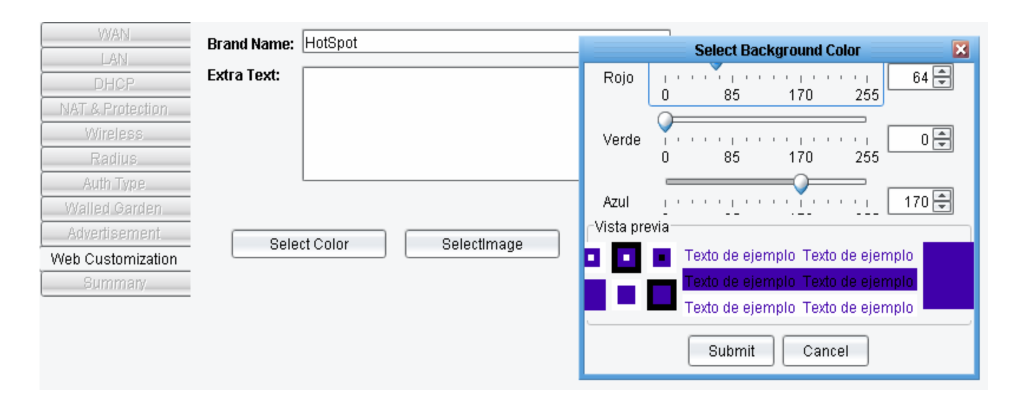


Figura 129. Personalización del web

En la pestaña **Summary** muestra un resumen de la configuración.

Click en **Submit** en la pestaña Summay.

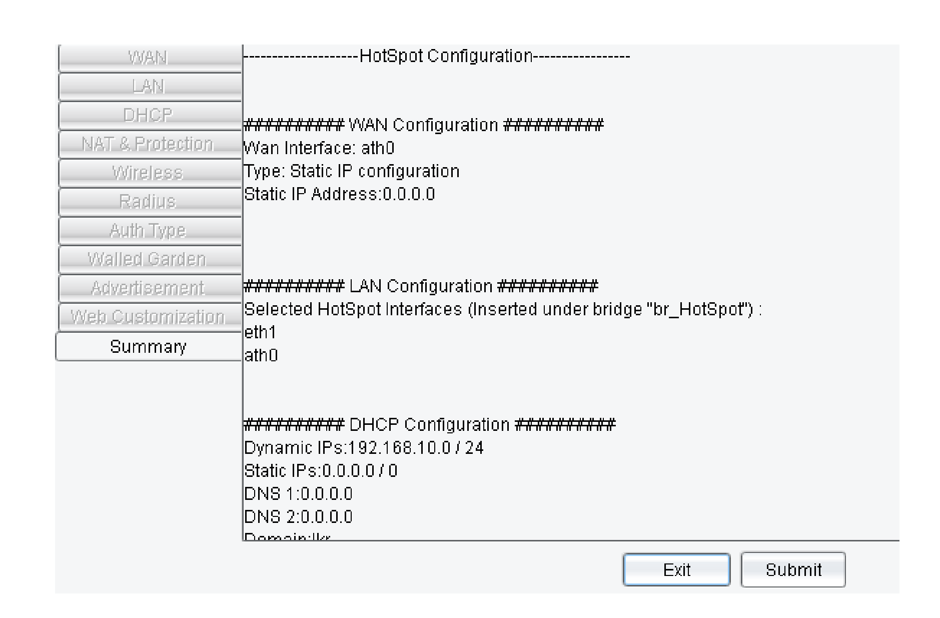


Figura 130. Resumen del Ejemplo

Click en **Exit**. El panel principal del **HotSpot** aparece.

Aunque la configuración se ha cargado, el Hotspot no se está ejecutando. (Status muestra: **Stopped [Parado]).** Para completar el procedimiento:

1. En **Admin MAC** escriba la dirección MAC del administrador.
2. Click en **Submit** para aplicar la configuración del HotSpot. La pestaña original del **HotSpot** aparece.
3. Para completar el proceso, seleccione **Enable HotSpot**.

Click en **Submit** para iniciar el HotSpot.

Nota: El *HotSpot asignará a su interfaz HotSpot la dirección IP: 192.168.0.1* La dirección IP del administrador será *192.168.0.2*

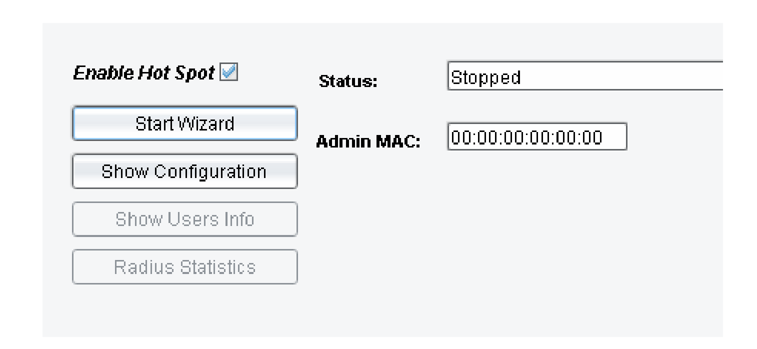


Figura 131. Iniciando el HotSpot - Ejemplo

Para actualizar el estado click en **Refresh**. Si **Status** muestra **Initializing**, inténtelo de Nuevo en unos cuantos minutos. Si **Status** muestra **Running** la inicialización se complete satisfactoriamente.

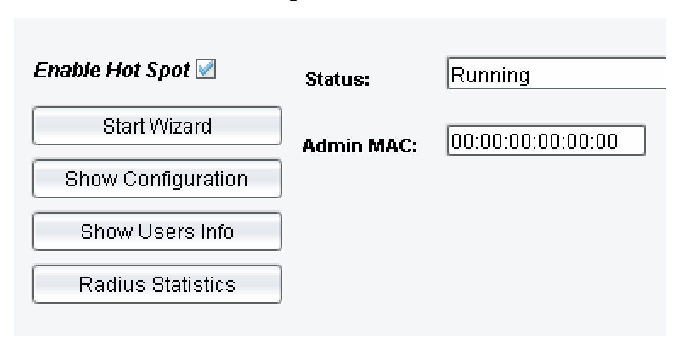


Figura132. Inicializando el HotSpot – Ejemplo

Retorne a la pestaña Network y note que la lista **Interface List** contiene un bridge **br_HotSpot** con las interfaces **eth1** y **ath0** debajo de este.

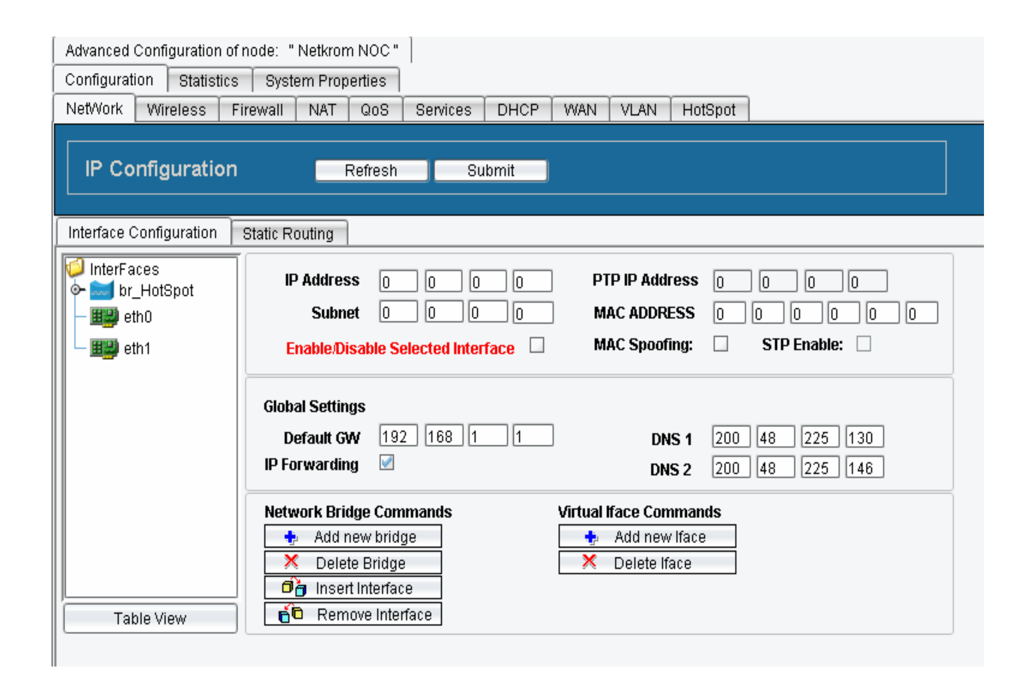
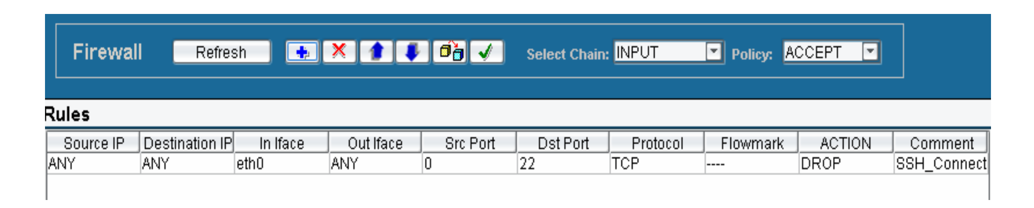


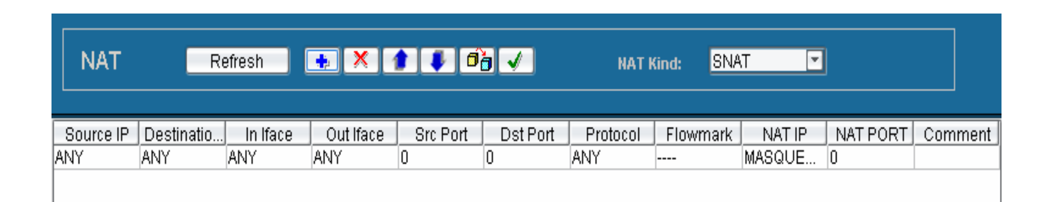
Figura 133. Panel de interfaces después de la inicialización del HotSpot - Ejemplo

Seleccione las pestañas **Firewall** y **NAT** y note que ellas también han sido inicializadas.



Source IP	Destination IP	In Iface	Out Iface	Src Port	Dst Port	Protocol	Flowmark	ACTION	Comment
ANY	ANY	eth0	ANY	0	22	TCP	----	DROP	SSH_Connect

Figura 134. Firewall del Ejemplo



Source IP	Destinatio...	In Iface	Out Iface	Src Port	Dst Port	Protocol	Flowmark	NAT IP	NAT PORT	Comment
ANY	ANY	ANY	ANY	0	0	ANY	----	MASQUE...	0	

Figura 135. NAT del Ejemplo

Si un usuario se conecta al HotSpot, se le asignará la siguiente dirección IP dinámica libre.

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : hotspot_domain
        IP Address. . . . . . . . . . . . : 192.168.0.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
```

Figura 136. El HotSpot le ha asignado una IP al usuario

Si este usuario ahora intenta acceder a internet, una página web de redirección se muestra a continuación.

11.5 Resolución de Problemas

11.5.1 No Se Puede Configurar la Interfaz Inalámbrica

- Verifique si usted ha seleccionado el canal y el ESSID.
- Si usted está ejecutando NETKROM OS con una licencia CPE, las interfaces wireless no pueden ser usadas con access points y el HotSpot no puede tener interfaces wireless HotSpot.

11.5.2 Error de DNS

- Si usted usa una dirección IP estática para la interfaz WAN, asegúrese de haber ingresado los parámetros correctos.
- Si usted usa asignación dinámica de IPs (clientes DHCP, PPPoE y PPTP), espere que la interfaz WAN establezca la conexión.

11.5.3 No Puede Obtener Una Dirección IP

- Verifique si las direcciones IP dinámicas son todas asignadas seleccionando **Show User Info**. Si se requieren más direcciones IP, reconsidere configurar una lista extendida de direcciones IP.
- Si la autenticación MAC está habilitada, verifique si su servidor RADIUS está operando y tiene conectividad con el HotSpot, o que los parámetros Radius sean los correctos (Secret Key, Ports).
- Verifique si el estado del Hotspot es running (Ejecutándose).

11.5.4 Se Obtiene Una Dirección IP pero No Se Puede Hacer Ping Al HotSpot

Verifique si el usuario está autenticado.

11.5.5 El HotSpot se está ejecutando, pero el servidor DHCP no se activa

El Hotspot usa su servidor DHCP incorporado; no hay ningún error de configuración.

11.5.6 Un usuario no está autenticado pero puede accede a internet

Verifique si el usuario está en el dominio Walled Garden.

11.5.7 El NETKROM NMS pierde conexión con el Hotspot

- Si usted accede al Hotspot a través de la interfaz WAN, asegúrese que la interfaz WAN ha establecido conectividad o usted no haya seleccionado HIGH Protection Level en la configuración del HotSpot (En esta situación la conexión entre el NNMS y la interfaz WAN se pierde).
- Si usted accede al Hotspot a través de la interfaz LAN del HotSpot y usted ha seleccionado HIGH Protection Level en la configuración del HotSpot, la conexión con el NNMS no se puede establecer.
- Si usted accede al HotSpot a través de la interfaz LAN del HotSpot, y usted ha configurado su dirección MAC como la MAC del administrador, habilite el cliente DHCP en su computadora. Si usted no puede obtener una dirección IP, configure su computadora con una dirección IP estática, la primera de las direcciones IP dinámicas (x.x.x.2) e intente de nuevo (Quizás el Hotspot se está inicializando).
- Si hay otra interfaz que no sea WAN ni LAN, intente conectarse a través de esta.

12. Servicios del Sistema

NETKROM puede ser configurado para ejecutar los siguientes servicios:

- Servicio **SNMP** (Simple Network Management Protocol)
- Servicio **HTTP** (Hyper-Text Transfer Protocol)
- Servicio **SSH** (Secure Shell Protocol)
- Servicio **NTP** (Network Time Protocol)

Para configurar los parámetros de los servicios, seleccione la pestaña **Services**, ubicado debajo de las pestañas **Advanced Configuration of Node, Configuration**.

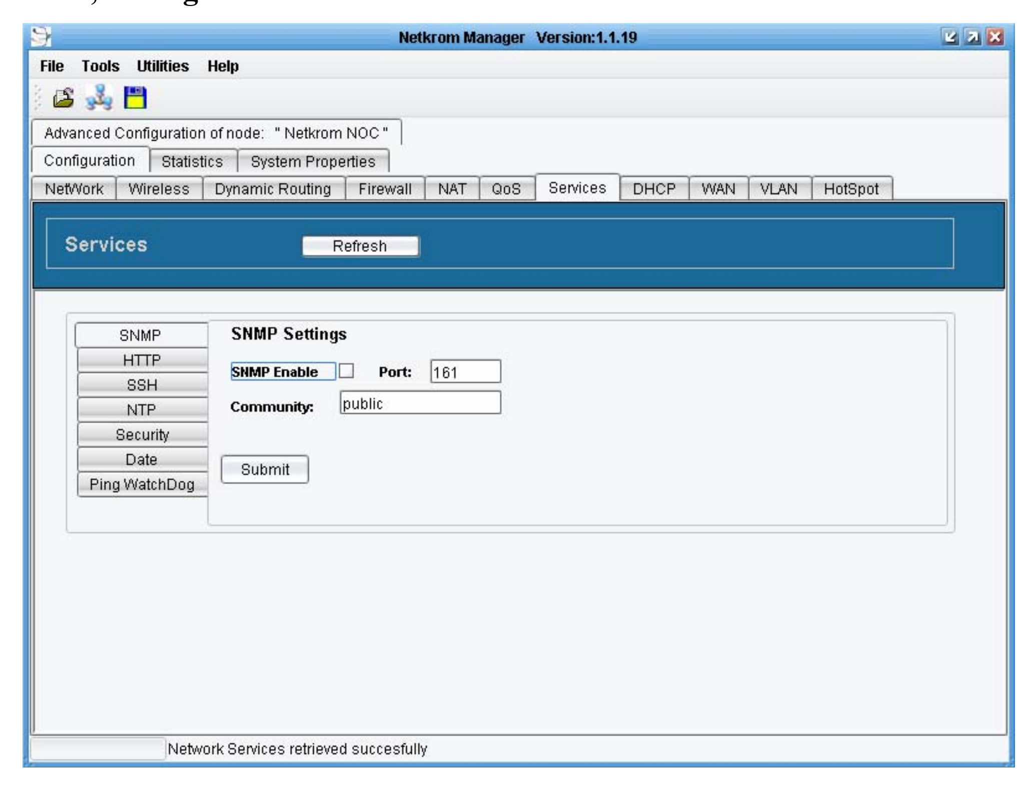


Figura 137. Pestaña Servicios

12.1 Configurando los Parámetros del SNMP

SNMP (Simple Network Management Protocol) es el protocolo más ampliamente usado para administrar Internet TCP/IP. Una estación de administración de red (NMS) o agente usa solicitudes SNMP en los dispositivos de red como routers y estaciones finales. Estos agentes mantienen una lista de variables y sus valores que describe el estado del dispositivo de red.

Estas variables pueden ser tablas de ruteo, direcciones IP de las interfaces, bytes transmitidos, etc. El conjunto de variables es descrito por una base de información de administración (MIB).

Cuando SNMP está habilitado, NETKROM responderá a las solicitudes SNMP (SNMP get, getnext, getbulk, walk).

Un nombre de comunidad puede ser configurado como una comunidad de solo lectura.

Para configurar **SNMP**, seleccione la pestaña **SNMP** debajo de la pestaña **Services**. Configure la pestaña SNMP como sigue:

SNMP Enable [Habilitar SNMP]

Seleccione la casilla **SNMP Enable** para habilitar el SNMP

Port [Puerto]

Contiene el Puerto que escucha las solicitudes SNMP (por defecto 161). Típicamente usted no tendrá que cambiar este valor.

Community [comunidad]

Contiene el nombre de la comunidad de solo lectura del servicio SNMP (por defecto: public). El servicio SNMP responderá a las solicitudes si el nombre de la comunidad esta apropiadamente configurado.

Submit [Enviar]

Click en **Submit** para aplicar la configuración.

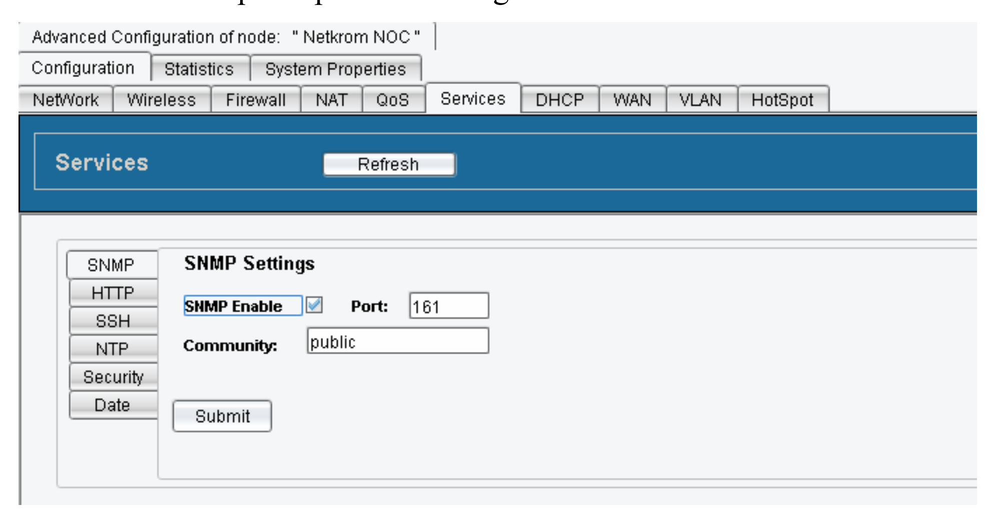


Figura 138. Configuración del servicio SNMP

12.2 Configurando los Parámetros HTTP

Los servidores Web son las computadoras que ejecutan sitios web, aceptando conexiones HTTP (Hyper-Text Transfer Protocol) desde buscadores web y entregando páginas web y otros archivos a ellos. Cuando HTTP está habilitado, NETKROM las solicitudes HTTP/HTTPS.

Para configurar **HTTP**, seleccione la pestaña **HTTP** debajo de la pestaña **Services**. Configure la pestaña HTTP como sigue:

HTTP Enable [Habilitar HTTP]

Seleccione la casilla **HTTP Enable** para habilitar el servicio HTTP.

Port [Puerto]

Contiene el Puerto que escuchará las peticiones de solicitud HTTP (por defecto 80). Generalmente usted no tendrá que cambiar este valor.

Upload SSL Certificate [Cargar Certificado SSL]

Click en **Upload SSL Certificate** para abrir y seleccionar una ventana y así cargar su certificado SSL para HTTPs. Un certificado por defecto se incluye en cualquier NETKROM.

Submit [Enviar]

Click en **Submit** para aplicar la configuración.

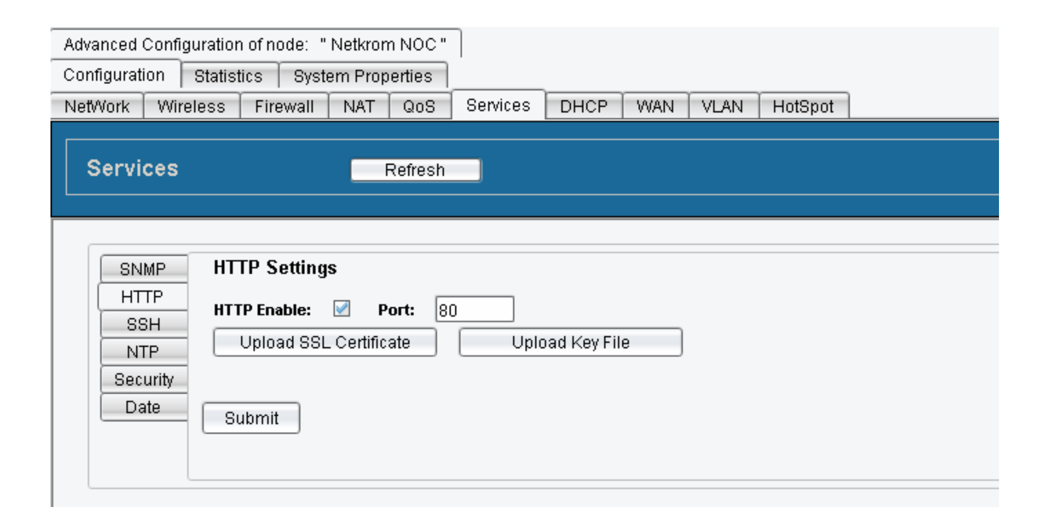


Figura 139. Configuración del servicio HTTP

12.3 Configurando los Parámetros del SSH

Para configurar **SSH**, seleccione la pestaña **SSH** que se encuentra debajo de la pestaña **Services**. Configure el SSH como sigue:

SSH Enable [Habilitar SSH]

Seleccione la casilla **SSH Enable** para habilitar el SSH

Port [Puerto]

Contiene el Puerto que escuchará las peticiones de solicitud SSH (por defecto 22). Generalmente usted no tendrá que cambiar este valor.

Submit [Enviar]

Click en **Submit** para aplicar la configuración.

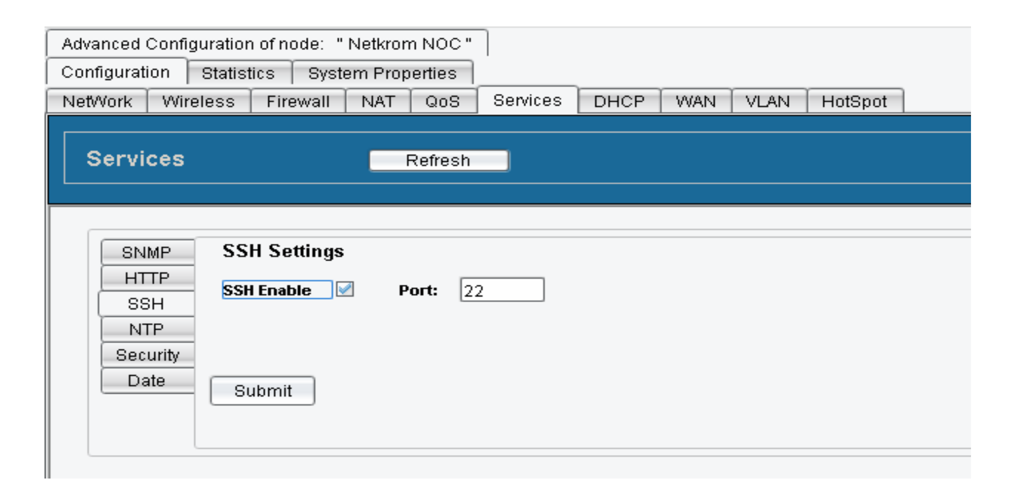


Figura 140. Configuración del servicio SSH

12.4 Configurando los Parámetros del NTP

El **Network Time Protocol (NTP)** es un sistema de sincronización de tiempo para relojes de computadora a través de Internet. Las principales características del NTP son las siguientes:

- Completamente automático, sincronización continua
- Adecuado para la configuración de una computadora o toda una red de computadoras.
- Tolerante a fallas y dinámicamente auto configurable.
- Basado en tiempo UTC, independiente de los husos horarios.
- Sincronización precisa (puede incluso alcanzar 1 milisegundo).

Cuando NTP está habilitado, NETKROM periódicamente enviará una solicitud a un servidor NTP configurado (basado en intervalos de tiempo) y ajustará el tiempo del sistema local de NETKROM.

Para configurar **NTP**, seleccione la pestaña **NTP** debajo de la pestaña **Services**. Configure la pestaña NTP como sigue:

NTP Enable [Habilitar NTP]

Seleccione la casilla **NTP Enable** para habilitar el NTP

Port [Puerto]

Contiene el Puerto que escuchará las peticiones de solicitud NTP (por defecto 123). Generalmente usted no tendrá que cambiar este valor.

Domain [Dominio]

Este campo contiene el nombre del dominio o dirección IP del servidor NTP.

Interval [Intervalo]

Contiene el intervalo en minutes entre dos solicitudes consecutivas (por defecto 60 minutos).

Submit [Enviar]

Click en **Submit** para aplicar la configuración.

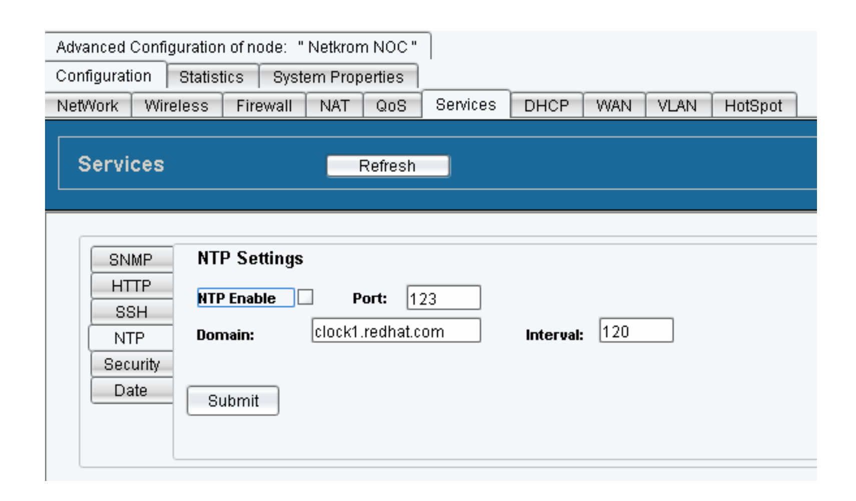


Figura 141. Configuración del servicio NTP

12.5 Configurando la Contraseña del Administrador

Para configurar la contraseña del administrador, seleccione la pestaña **Security** debajo de la pestaña **Services**. Configure la pestaña Security como sigue:

Old Password [Contraseña Antigua]

Escriba la contraseña actual en **Old Password**. La contraseña por defecto es: *admin*

New Password [Contraseña Nueva]

Escriba la nueva contraseña en **New Password**. La nueva contraseña debe tener al menos 8 carácteres y no más de 63 carácteres.

Re-type [Re Escribir]

Vuelva a escribir la nueva contraseña en **Retype.**

Submit [Enviar]

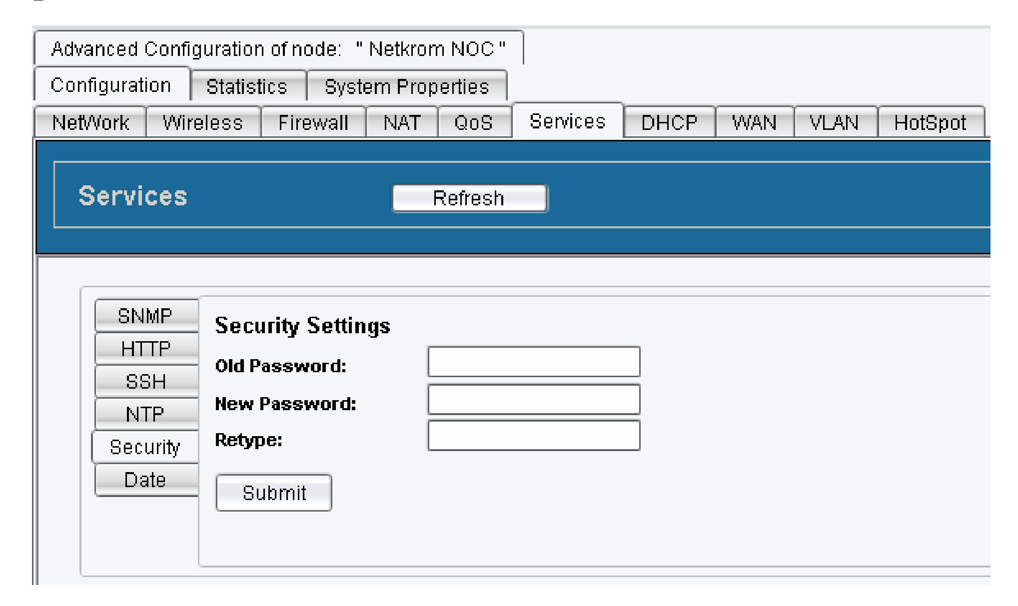


Figura 142. *Configuración de la contraseña del administrador*

Click en **Submit** para aplicar la configuración.

13. Monitoreo y Estadísticas

El motor de búsqueda avanzado de estadísticas del NETKROM OS, en combinación con funcionalidades gráficas del NETKROM NMS, permite al administrador ahondar en resultados de tiempo real, identificando nodos de alto ancho de banda y posibles cuellos de botellas.

Algunas características son disponibles desde el **Node Shortcut Menu.** Otras están ubicadas debajo de las pestañas **Advanced Configuration of Node, Configuration**.

13.1 Usando la Ventana Status Info

La ventana **Status Info** proporciona toda la información mostrada en el panel inferior de la pestaña **Network Topology**, con la adición de un campo extra editable el cual es usado para configurar el nombre del host del nodo. La información mostrada es útil en casos donde la unidad de administración está oculta detrás de NAT y comunicaciones sin conexión (como el protocolo de sondeo de NETKROM y SNMP) pueden no ser iniciados.

Para ver el Status Info, click en **Open Status Window** del **Node Shortcut Menu.**

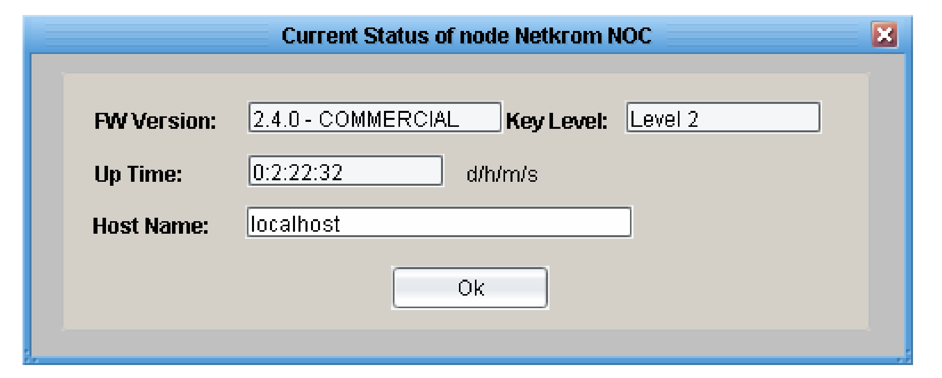


Figura 143. Estado actual del nodo

13.2 Usando el Gráfico de Throughput

Esta herramienta suministra un gráfico en tiempo real del tráfico transmitido y recibido de cada interfaz de red. Monitoreando el rendimiento y analizando los datos usted puede empezar a ver patrones en los datos que le ayudarán a ubicar cuellos de botella. Después de haber ubicado los cuellos de botella usted puede hacer cambios para mejorar el rendimiento. Los cuellos de botella pueden ocurrir en cualquier parte, por lo tanto es importante tener información base de este tipo.

Para ver el **Current Throughput Graph**, click en **Current Throughput** del **Node Shortcut Menu.**

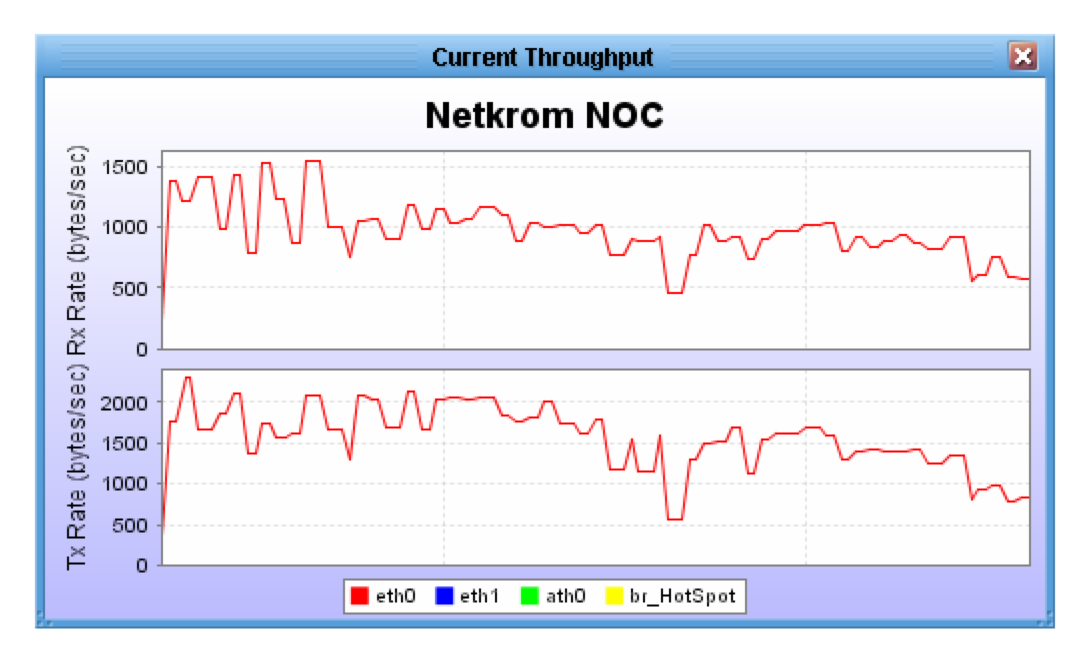


Figura 144. Ventana Current Throughput

13.3 Viendo las Estadísticas de los Paquetes

La pestaña **Packet Stats** contiene información concerniente a las estadísticas de paquetes por interfaz.

Para ver las estadísticas de los paquetes, seleccione la pestaña **Packet Stats** debajo de las pestañas **Advanced Configuration, Statistics, Network**.

Interface [Interfaz]

Seleccione la interfaz por la cual usted desea ver las estadísticas de la lista desplegable.

Refresh [Refrescar]

Click en **Refresh** para actualizar el gráfico.

Reset

Click **p**ara resetear.

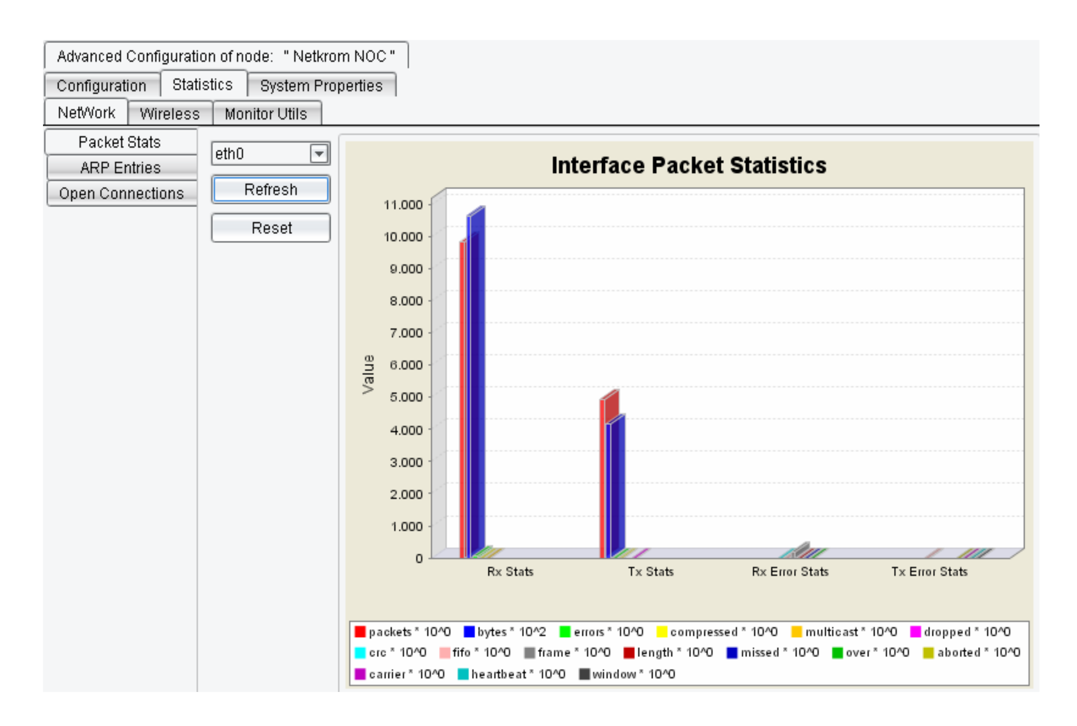


Figura 145. Estadística de paquetes por interfaz

13.4 Viendo la Tabla ARP

La tabla ARP muestra las IPs asociadas a las direcciones MAC
Para ver la tabla ARP, seleccione la pestaña **ARP Entries** debajo de la pestaña **Network**.

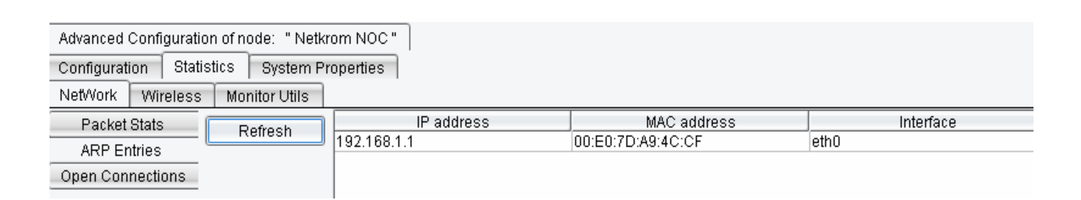


Figura 146. Tabla ARP

13.5 Viendo la Lista de Conexiones Abiertas

La pestaña **Open Connections** muestra todas las conexiones entrantes y salientes y todos los puertos abiertos, ayudando al administrador a detector actividad de los hosts. Las conexiones abiertas pueden ser clasificadas en orden ascendente y descendente por columna haciendo click en el encabezado de la tabla correspondiente.

Para ver la lista de conexiones abiertas, seleccione la pestaña **Open Connections** debajo de las pestañas **Advanced Configuration, Statistics, Network**.

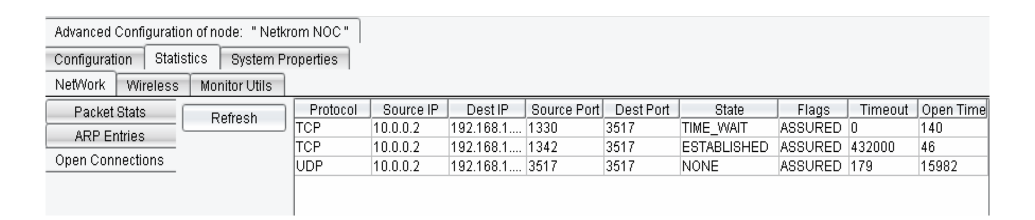


Figura 147. Pestaña de conexiones abiertas

Refresh [Actualizar]

Click en **Refresh** para actualizar la lista de conexiones abiertas.

13.6 Usando las Utilidades de Monitoreo

La pestaña **Monitor Utilities** suministra una interfaz de usuario para implementar dos utilidades de red útiles: **Ping (ICMP)** y **Traceroute**. Para accede a estas utilidades, seleccione la pestaña **Monitor Utilities** debajo de las pestañas **Advanced Configuration, Statistics**. La pestaña **Monitor Utils** tiene dos sub pestañas: la pestaña **ICMP Util** y la pestaña **Trace Route**.

13.6.1 Ping (Utilidad ICMP)

La pestaña **ICMP Util** suministra una herramienta conveniente para iniciar comandos Ping. Ping envía solicitudes ICMP a la dirección que usted especifica y muestra las respuestas recibidas y su tiempo respectivo. Cuando la utilidad termina muestra un resumen en un gráfico dando el promedio del tiempo de respuesta y el porcentaje de paquetes perdidos. Esta utilidad puede ser usada para determinar si hay problemas de conectividad entre dos hosts.



Figura 148. Pestaña ICMP Utility

Para configurar y usar el ICMP Utility, seleccione la pestaña **ICMP Util**, configure el destino y el tamaño del paquete, luego use **Empezar, Parar** y **Limpiar** como sigue:

Destination [Destino]

Escriba la dirección IP del nodo al cual usted desea hacer ping.

Packet Size [Tamaño del Paquete]

Escriba el número de bytes que van a ser enviados en cada paquete.

Start [Empezar]

Click en **Start** para iniciar el comando Ping. El software hará Ping repetidamente a la dirección de destino. La ventana mostrará el número de bytes, dirección de origen, tiempo de vida (TTL), tiempo de respuesta, % de paquetes perdidos, y tiempo promedio.

Stop [Parar]

Click en **Stop** para terminar el proceso Ping. La sesión Ping terminará y una ventana aparecerá mostrando las estadísticas de paquetes en un gráfico.

Clear [Limpiar]

Click en **Clear** para limpiar los datos de la ventana. Los datos pueden ser limpiados mientras la sesión Ping se está ejecutando.

13.6.2 Usando Traceroute

La pestaña **Traceroute** proporciona una herramienta conveniente para iniciar los comandos Trace Route.

Traceroute es una utilidad que almacena la ruta (el gateway específico en cada salto) a través de Internet entre su nodo NETKROM y un destino específico. También calcula y muestra la cantidad de tiempo de cada salto. Traceroute es una herramienta para entender donde se encuentras los problemas de la red.

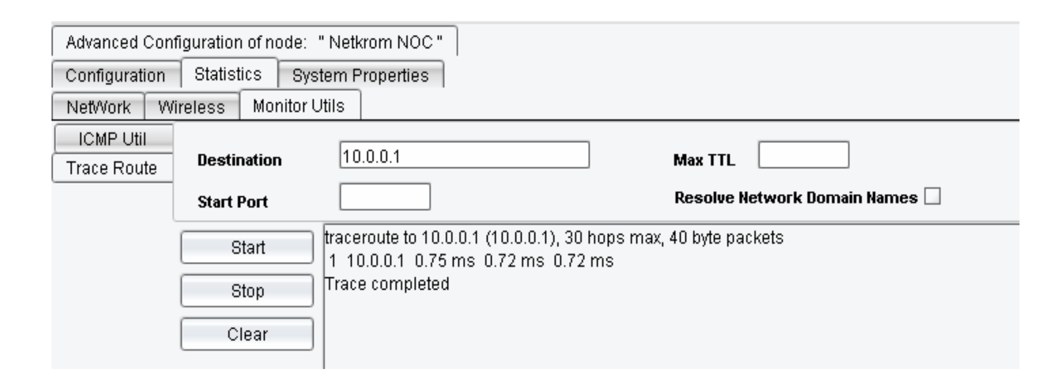


Figura 149. Pestaña Traceroute

Para configurar y usar la utilidad Trace Route, seleccione la pestaña Trace Route, configure los campos requeridos, luego use los botones como sigue:

Destination [Destino]

Escriba la dirección IP del host al cual usted desea hacer el Traceroute.

Start Port [Puerto]

Escriba el número de puerto.

Max TTL [Máximo Tiempo de Vida]

Escriba el máximo tiempo de vida.

Resolve Network Domain Names [Resolver Nombres de Dominio]

Selecciónelo para que la utilidad incluya los nombres del dominio de cada dirección IP de la lista.

Start [Empezar]

Click para iniciar el proceso Trace Route. El software trazará la ruta a la dirección de destino. La ventana mostrará el número de satos máximos, tamaño del paquete y tiempo de enlace.

Stop [Parar]

Click para terminar el proceso Trace Route. La sesión Traceroute terminará.

Clear [Limpiar]

Click para limpiar los datos de la ventana.

13.7 Viendo las Propiedades del Sistema

La pestaña **System Properties** proporciona información sobre el CPU y memoria del nodo seleccionado. Para accede a **System Properties,** seleccione la pestaña **System Properties** debajo de la pestaña **Advanced Configuration.**

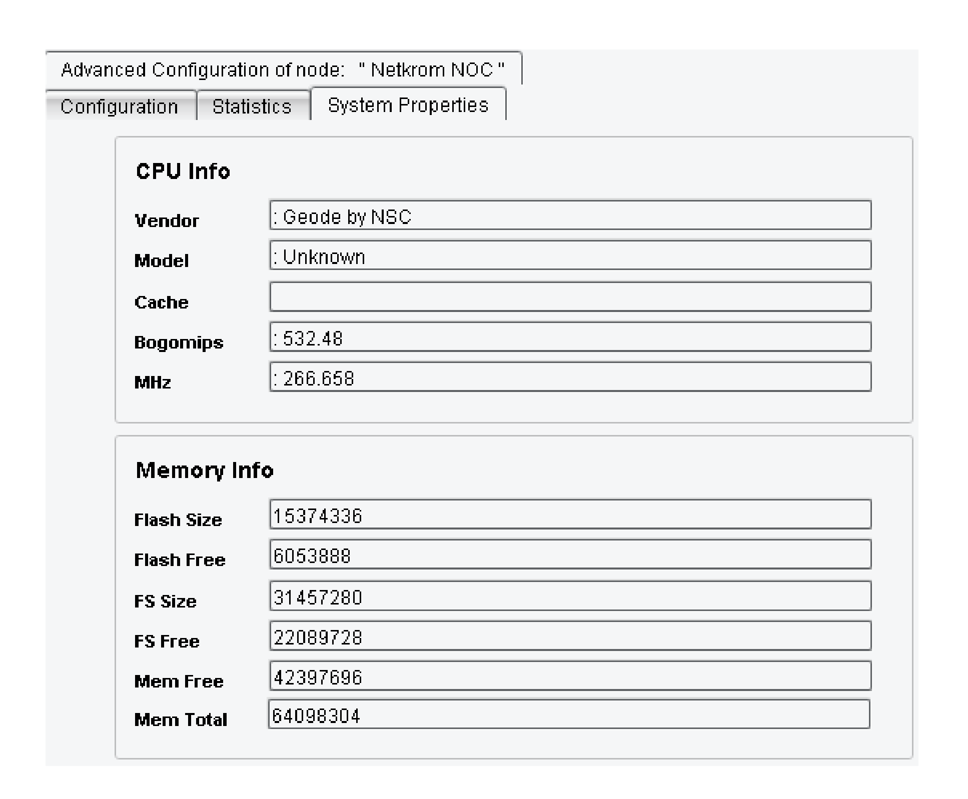
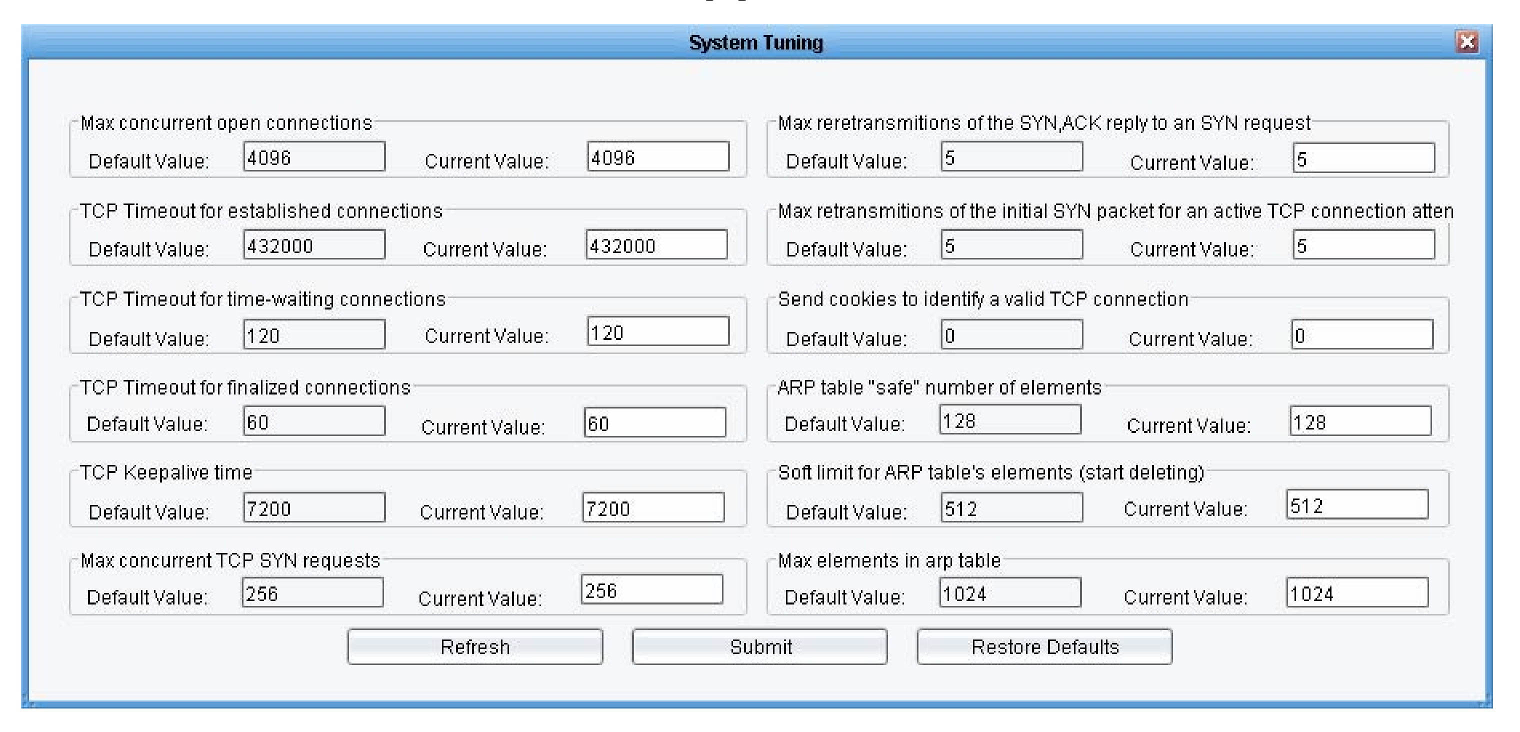


Figura 150. Propiedades del Sistema

Para actualizar los datos, click en **Refresh**.

14. Ajuste del Sistema

System Tune le permite maximizar el rendimiento de aplicaciones específicas. Usando estos parámetros usted será capaz de configurar parámetros avanzados del stack TCP, hacer ajustes avanzados para tener un mejor control de sus enlaces, restringir y limitar ciertas solicitudes de comunicación con su equipo inalámbrico.



Max Concurrent Open Connections

Este campo contiene el máximo número de conexiones abiertas al mismo tiempo.

TCP Timeout for Established Connections

Contiene el máximo valor permitido de una implementación TCP para establecer un tiempo de espera, medido en milisegundos.

TCP Timeout for time-waiting connections

Contiene el máximo valor permitido por una implementación TCP para el time-waiting del tiempo de espera, medido en milisegundos.

TCP Timeout for finalized connections

Contiene el máximo valor permitido por una implementación TCP para finalizar el tiempo de espera, medido en milisegundos.

TCP Keepalive time

Contiene el tiempo de una conexión TCP que va ser mantenida. El concepto de keepalive es muy simple: cuando usted configure una conexión TCP, usted asocia un conjunto de temporizadores. Algunos de estos temporizadores trata el procedimiento de keepalive. Cuando el temporizador de keepalive llega a cero, usted envía al otro punto un paquete keepalive sin datos y la bandera de ACK activada. Usted puede hacer esto ya que las especificaciones TCP/IP, como una especie de duplicado ACK, y el host remoto no tendrá argumentos, como TCP es un protocolo de flujo orientado. De otro lado, usted recibirá una respuesta desde el host remoto (el cual no necesita soportar el keepalive de todo, solo TCP/IP), sin datos y ACK configurado.

Si usted recibe una respuesta al keepalive de prueba, usted puede afirmar que la conexión está todavía bien y ejecutándose sin preocupaciones sobre la implementación del nivel del usuario. De hecho, TCP permite manejar un flujo, no paquetes y un paquete de cero de longitud no es dañino para el programa del usuario.

Este procedimiento es útil ya si otros puntos pierden conexión (por ejemplo por reinicio) usted notará que la conexión está rota incluso si usted no tiene tráfico ahí. Si las pruebas del keepalive no son contestadas por su punto, usted puede afirmar que la conexión no puede ser configurada válida y luego tomar la acción correcta.

Max concurrent TCP SYN requests

Contiene el número de intentos de conexión simultáneos.

Max reretransmitions of the SYN/ACK reply to an SYN request

Este parámetro define el máximo número de retransmisiones que un host remoto responderá (SYN/ACK) si no recibe respuesta desde el host transmisor (syn request). Este proceso es usado para proteger el enlace de DDoS.

Send cookies to identify a valid TCP connection

ARP table "safe" number of elements

Muestra el número de MACs que pueden ser consideradas como seguras.

Soft limit for ARP table's elements (Empezar a borra)

Contiene el número a la cual el sistema empieza a eliminar entradas ARP de la tabla hasta que alcance l número seguro de elementos.

Max elements in arp table

Contiene el máximo número de entradas para la tabla MAC

15. Soporte de MRTG

Multi Router Traffic Grapher, o **MRTG**, es una helos enlaces de red. MRTG genera páginas HTML conteniendo imágenes GIF las cuales proporcionan una representación visual de este tráfico.

Un cliente MRTG el cual es soportado por NETKROM NMS usa el paquete proveído por JRobin (http://www.jrobin.org/utilities/MRTGdemo.html).

Para usar el **MRTG**, seleccione **MRTG** debajo del menú **Utilities**.

15.1 Usando MRTG

Para implementar el MRTG, extraiga los archives requeridos en un servidor web con soporte de java e inicie ejecutando el siguiente comando: "java – jar MRTG-server-1.4.0.jar".

Usando MRTG

- Después de iniciar el servidor MRTG satisfactoriamente, en el menú **Utilities** seleccione **MRTG**. El cliente MRTG incorporado será invocado y un mensaje aparece solicitando la dirección IP del servidor MRTG.
- Escriba la dirección IP del servidor MRTG. Después de la conexión exitosa los nodos pueden ser insertados en la lista de monitoreo.
- En cada inserción del nodo el usuario se le presentara una lista de todas las interfaces disponibles. El usuario puede seleccionar una o más interfaces para monitorear.

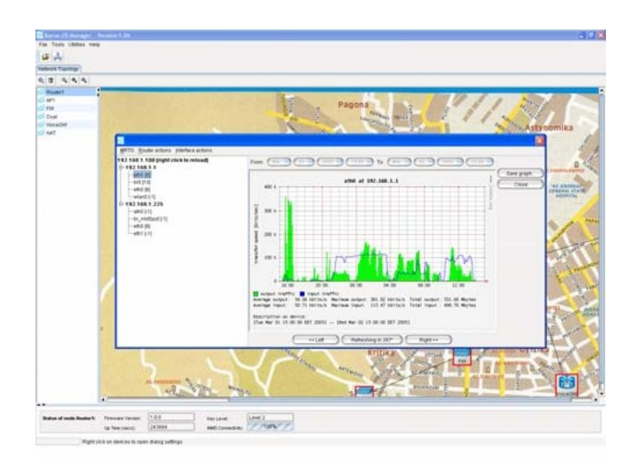


Figura 151. MRTG

NOTA: *El servidor JRobin MRTG usa SNMP para almacenar información lo cual significa que el agente SNMP tiene que habilitarse en el nodo monitoreado.*

16. WISP Easy Wizard

El **WISP Easy Wizard** es una extensión del NETKROM NMS que proporciona una manera conveniente y fácil de instalar nodos NETKROM.

Para iniciar el WISP Easy Wizard, en **Node Shortcut Menu**, seleccione **WISP Easy Wizard (WEW).** La ventana **WISP Easy Wizard (WEW)** aparece y muestra algunas instalaciones típicas WISP.

Seleccione uno de los modos de funcionamientos disponibles. Una breve descripción se muestra es la esquina superior izquierda de la ventana cuando el cursor se pone encima de una imagen.

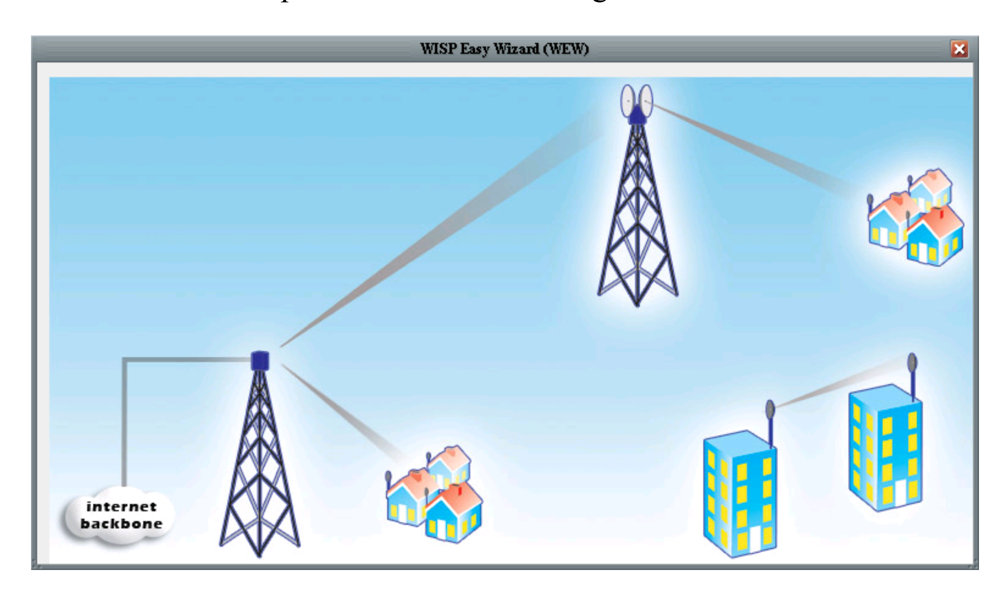


Figura 152. WISP Easy Wizard

Escenarios de configuración disponibles:

- **Backhaul AP**
- **Repetidor AP**
- **Enlace Punto a Punto**
- **Instalación CPE**

Seleccionar el modo que más se asemeja a su objetivo le permite accede a un procedimiento de configuración paso por paso simplificado, el cual le guía a través de todo el proceso de configuración.

Después de completar el wizard, usted puede ajustar la configuración aplicada manualmente como se ha descrito en los capítulos anteriores.

NOTA: Después de la aplicación exitosa de la configuración vía WEW, la IP actual se mantiene para evitar pérdida de conectividad con el dispositivo. Si el usuario no requiere esa IP nunca más, se recomienda eliminarla mediante la eliminación de la interfaz virtual correspondiente.

17. Índice